Recording Component (RC-E)

User Manual

© 2012 On-Net Surveillance Systems Inc.

On-Net Surveillance Systems, Inc.
One Blue Hill Plaza, 7th Floor, PO Box 1555
Pearl River, NY 10965
Phone: (845) 732-7900 | Fax: (845) 732-7999
Web: www.onssi.com

00081512-0945-RC-5_5.0-OC3.5.0.77_v01

Legal Notice

This product manual is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

© 2002-2012 On-Net Surveillance Systems, Inc. All rights reserved. OnSSI and the 'Eye' logo are registered trademarks of On-Net Surveillance Systems, Inc. Ocularis, Ocularis Client, Ocularis Client Lite, Ocularis Video Synopsis, NetEVS, NetDVMS, NetDVR, ProSight, NetGuard, NetGuard-EVS, NetSwitcher, NetMatrix, NetCentral, NetTransact, NetPDA and NetCell are trademarks of On-Net Surveillance Systems, Inc. All other trademarks are property of their respective owners.

On-Net Surveillance Systems, Inc. reserves the right to change product specifications without prior notice.

Patents Applied For in the U.S. and Abroad

Contents

Introductions 7
Product Overview, RC-E 7
About Updates 7
The RC-E Server (Management Server) 7
The RC-E Recording Server 8
The Management Client (RC-E Manager) 8
The Download Manager 8
System Requirements 9
Computer Running Management Server 9
Computer Running Recording Server or Failover Server 9
Computer Running Management Client 10
Computer Running Log Server 10
Active Directory 10
Navigating the Built-in Help System 11
Installation and Removal 12
Installation Overview 12
Installing RC-E on Virtual Servers 12
Install Management Server 13
Step 1: Internet Information Services 14
Step 2: RC-E Management Server Database 15
Step 3: RC-E Management Server 15
What's Next? 17
Install System Components 17
Part I—Downloading the Installer 17
Part II—Installing the Component 18
Recording Servers 18
Failover Servers 20
Management Client 21
Specify Recording Server Setup Parameters 21
Install Log Server (Custom) 21
Installing Log Server 22
Important Port Numbers 23
List of Ports Used by RC-E 23
Multiple Management Servers (Clustering) 24
Prerequisites for Installing OnSSI RC-E in a Cluster 25
Installing RC-E in a Cluster 25
Upgrading RC-E in a Cluster 26
Multiple Recording Server Instances 26
Installing Multiple Recording Server Instances 27
Remove System Components 27
Removing Management Server 27
Removing Download Manager and Log Server 27
Removing Management Client 28
Removing Recording Server 28
Upgrade from Previous Version 28
Prerequisites 28
Upgrading the Management Server 29
Upgrading Recording Servers 29
Upgrading a Management Client 30
Upgrading Video Device Drivers 30
Installation Troubleshooting 30

Issue: Automatic IIS Installation for Mgmt. 30
Issue: Recording Server Startup Fails due to Port Conflict 31
Issue: Changes to SQL Server Location Prevents Database Access 33
Issue: Insufficient Continuous Virtual Memory Fails Installation 33
Issue: Multi-domain Environments; One-way Trusts not Working 33
Management Client (RC-E Manager) 34
Management Client (RC-E Manager) Overview 34
Management Client's Elements 34
Site Navigation Pane and Federated Hierarchy Pane 34
Menu Bar 35
Toolbar 35
Memory Indicator 35
Panes Overview 36
Menu and Tool Bars 36
Overview Pane 36
Preview Pane 36
Properties Pane 36
Site Navigation Pane and Federated Hierarchy Pane 37
Basics 37
Get Started 37
Log in to the Management Client 39
Management Client Menu Overview 40
Customize the Management Client's Layout 41
Activate Licenses 43
Manage Licenses 45
Remote Connect Services 46
About Remote Connect Services 46
Axis One-Click Camera Connection Properties 48
Servers 49
Add Hardware (Cameras, etc.) 49
Manage Hardware 53
About Storage and Archiving 56
Manage Recording Servers 60
Manage Multicasting 70
Manage Public Addresses 72
Servers and Clients Require Time-Synchronization 73
Devices 75
About Devices 75
Client 108
About Clients 108
Manage View Groups 108
Rules and Events 109
About Rules and Events 109
Actions and Stop Actions Overview 110
Create Typical Rules 116
Default Rules 126
Events Overview 128
Manage Rules 133
Manage Time Profiles 138
Manage Day Length Time Profiles 140
Manage Notification Profiles 141
Manage User-defined Events 143
Security 145
About Security 145
About Roles 145
Manage Roles 147

Manage View Groups 154
System Dashboard *156*
About System Dashboard 156
About System Monitor 156
About Current Task 157
About Configuration Report 157
Server Logs *158*
Manage Logs 158
RC-C *162*
Manage RC-C Servers 162
Registered Services *165*
Manage Network Configuration 165
Manage Registered Services 165
Important Prerequisites When Running Federated Sites *166*
Options *168*
Options 168
AVI Compression Settings 170
Outgoing SMTP Mail Server Settings 171
Manage Local IP Address Ranges 171
OnSSI Federated Architecture 173
OnSSI Federated Architecture Overview *173*
Licensing of OnSSI Federated Architecture 173
Basic Rules of Federated Sites 174
Principles for Setting Up Federated Sites 174
The Administrator Role and Federated Sites 174
Possibilities and Constrains of Federated Sites 175
Frequently Asked Questions to Federated Sites 175
Federated Sites Example Scenario—Limestone City 177
Manage OnSSI Federated Architecture *177*
Expand/Collapse 178
Site Navigation Pane 178
Right-clicking is not Selecting! 178
Context Menu 178
Adding a Site to the Hierarchy 178
Accepting Inclusion in the Hierarchy 179
Connecting to Another Site in the Hierarchy 180
Detaching a Site from the Hierarchy 180
Refreshing the Site Hierarchy 181
Renaming a Site 181
Setting the Site Properties 181
Backup, Restore and Move System Configuration 183
Scheduled Backup & Restore of System Configuration *183*
Flushing the SQL Server Transaction Log 183
Prerequisites 183
Scheduled Back Up of System Configuration 183
Backing Up Log Server Database 184
Restoring System Configuration (From Scheduled Back Up) 184
Manual Backup & Restore of System Configuration *185*
Select Shared Backup Folder 185
Manual Back Up of System Configuration 185
Restoring System Configuration (From Manual Back Up) 186
Move System Configuration to New Management Server *186*
Copying System Configuration from Old Server (Step 1) 188
What Happens while the Management Server Is Unavailable? 188
Copying Log Server Database 188
Installing New Management Server on New Server (Step 2) 189

Copying/Restoring System Configuration to New Server (Step 3) 189
Device Drivers 190
Manage and Remove Video Device Drivers 190
Making New Video Device Driver Versions Available for Installation 190
Installing Video Device Drivers 190
Removing Video Device Drivers 190
Failover Servers 191
Failover Server Service Administration 191
Starting and Stopping the Failover Server Service 191
Changing the Management Server Address 191
Viewing Status Messages 191
Viewing Version Information 192
Manage Failover Servers 192
Installing Failover Servers 193
Adding and Grouping Failover Servers 193
Enabling Failover Servers 194
Editing Failover Server Properties 194
Assigning Failover Servers to Recording Servers 195
Frequently Asked Questions 195
Failover-Related Events 196
Database Corruption 197
Protect Databases from Corruption 197
Power Outages: Use a UPS 197
Windows Task Manager: Be Careful when Ending Processes 197
Hard Disk Failure: Protect Your Drives 197
Services Administration 198
Management Server Service and Recording Server Service 198
Accessing the Server Service 198
Starting the Server Service 198
Stopping the Server Service 198
Changing Recording Server Settings 199
Viewing Status Messages 199
Viewing Version Information 199
Work with Recording Server Settings in details 199
Virus Scanning 200
Virus Scanning Information 200
SNMP 201
SNMP Support 201
Installing the SNMP Service 201
Configuring the SNMP Service 201
Daylight Saving Time 202
Daylight Saving Time 202
Spring: Switch from Standard Time to DST 202
Fall: Switch from DST to Standard Time 202
Contact Information 203

Introductions

Product Overview, RC-E

The RC-E recorder, part of Ocularis ES, is a fully distributed solution, designed for large multi-site and multiple server installations requiring 24/7 surveillance, with support for devices from different vendors. The solution offers centralized management of all devices, servers, and users, and empowers an extremely flexible rule system driven by schedules and events.

While Ocularis contains multiple components, RC-E also contains its own components.

RC-E consists of the following main elements:

- The **management server** - the center of your installation (RC-E Server)
- One or more **recording servers** (RC-E Recorder)
- One or more **Management Clients** (RC-Manager),which are unlicensed and can be downloaded and installed for free (as many times as needed).
- A **Download Manager**

Finally, RC-E handles an unlimited number of cameras, servers, and users—across multiple sites if required.

About Updates

OnSSI regularly release service updates for our products, offering improved functionality and support for new devices.

If you are an RC-E system administrator, it is recommended that you check the OnSSI website for updates at regular intervals in order to make sure you are using the most recent version of RC-E.

The RC-E Server (Management Server)

What? Stores the surveillance system's configuration in a relational database, either on the management server computer itself or on a separate SQL Server on the network. Also handles user authentication, user rights, etc. To enhance system performance, several management servers can be run under OnSSI Federated Architecture (see "OnSSI Federated Architecture Overview" on page 173).

Where? Runs as a service, and is typically installed on a dedicated server.

- **What is provided with the management server?** When installing the management server if you select Typical Management Server Installation (see "Typical" on page 16), you will also install:

  The **log server**

  - **What?** Provides the necessary functionality for logging information from your RC-E installation.
  - **Where?** Usually installed on the same server as the management server and runs as a service.

The RC-E Recording Server

What? Used for recording video and for communicating with cameras and other devices. In large installations, more than one recording server is often used on the surveillance system. Failover servers can be set up to take over if a recording server becomes temporarily unavailable.

Where? Recording servers as well as failover servers run as services, and are typically installed on separate servers rather than on the management server itself.

The Management Client (RC-E Manager)

What? Feature-rich administration client for configuration and day-to-day management of the system. Available in several languages.

Where? Typically installed on the surveillance system administrator's workstation or similar.

The Download Manager

What? Lets surveillance system administrators manage which RC-E -related components your organization's users will be able to access from a targeted web page generated by the management server.

Where? Automatically installed on the management server during RC-E installation process.

System Requirements

IMPORTANT: RC-E no longer supports Microsoft® Windows® XP (however, clients can still be run/accessed from computers with Windows XP Professional).

It is recommended to have the Microsoft Active Directory (see "Manage Users and Groups" on page 145)® in place before you install RC-E. If you add the management server to the Active Directory after installing RC-E, you must re-install the management server, and replace users with new users defined in the Active Directory.

The following are *minimum* requirements for the computers used in an RC-E solution:

Computer Running Management Server

- **CPU:** Intel® Xeon® , minimum 2.0 GHz (Dual Core recommended)
- **RAM:** Minimum 1 GB (2 GB or more recommended)
- **Network:** Ethernet (1 Gbit recommended)
- **Graphics Adapter:** Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color
- **Hard Disk Type:** E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
- **Hard Disk Space:** Minimum 50 GB free (depends on number of servers, cameras, rules, and logging settings)
- **Operating System:** Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008 (32 or 64 bit), Microsoft® Windows® Server 2003 (32 or 64 bit).

  Furthermore, to run clustering/failover servers, a Microsoft® Windows® Server 2003/2008 Enterprise or Data Center edition is needed.
- **Software:** Microsoft .NET 3.5 SP1 and .NET 4.0 and Internet Information Services (IIS) 5.1 or newer.

Computer Running Recording Server or Failover Server

- **CPU:** Dual Core Intel Xeon, minimum 2.0 GHz (Quad Core recommended)
- **RAM:** Minimum 1 GB (2 GB or more recommended)
- **Network:** Ethernet (1 Gbit recommended)
- **Graphics Adapter:** Onboard GFX, AGP, or PCI-Express, minimum 1024 x 768, 16-bit color
- **Hard Disk Type:** E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
- **Hard Disk Space:** Minimum 100 GB free (depends on number of cameras and recording settings)
- **Operating System:** Microsoft® Windows® 7 Ultimate (32 bit or 64 bit), Microsoft® Windows® 7 Enterprise (32 bit or 64 bit), Microsoft® Windows® 7 Professional (32 bit or 64 bit), Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008 (32 or 64 bit), Microsoft® Windows® Vista® Business (32 or 64 bit), Microsoft® Windows® Vista Enterprise (32 or 64 bit), Microsoft® Windows® Vista Ultimate (32 or 64 bit) or Microsoft® Windows® Server 2003 (32 or 64 bit).
- **Software:** Microsoft .NET 4.0 Framework.

IMPORTANT: When formatting the hard disk of a recording/failover server device, it is important to change its *Allocation unit size* setting from 4 to 64 kilobytes. This is to significantly improve recording performance of the hard disk. You can read more about allocating unit sizes and find help at http://support.microsoft.com/kb/140365/en-us (see http://support.microsoft.com/kb/140365/en-us - http://support.microsoft.com/kb/140365/en-us).

Computer Running Management Client

- **CPU:** Intel Core2TM™ Duo, minimum 2.0 GHz
- **RAM:** Minimum 1 GB
- **Network:** Ethernet (100 Mbit or higher recommended)
- **Graphics Adapter:** AGP or PCI-Express, minimum 1024 x 768 (1280 x 1024 recommended), 16-bit color
- **Hard Disk Space:** Minimum 100 MB free
- **Operating System:** Microsoft® Windows® 7 Professional (32 bit or 64 bit*), Microsoft® Windows® 7 Enterprise (32 bit or 64 bit*), Microsoft® Windows® 7 Ultimate (32 bit or 64 bit*), Microsoft® Windows® Vista Ultimate (32 bit or 64 bit*), Microsoft® Windows® Vista Enterprise (32 bit or 64 bit*), Microsoft® Windows® Vista Business (32 bit or 64 bit*), Microsoft® Windows® Server 2008 (32 bit or 64 bit*), Microsoft® Windows® Server 2008 R2 (64 bit) or Microsoft® Windows® Server 2003 (32 bit or 64 bit*).

  * Running as a 32 bit service/application

- **Software:** Microsoft .NET 4.0 Framework, DirectX 9.0 or newer, and Windows Help (WinHlp32.exe) which you can download from http:// www.microsoft.com/downloads/ **(see http://www.microsoft.com/downloads/ -** http://www.microsoft.com/downloads/**).**

Computer Running Log Server

- **CPU:** Intel® Xeon® , minimum 2.0 GHz (Dual Core recommended)
- **RAM:** Minimum 1 GB (2 GB or more recommended)
- **Network:** Ethernet (1 Gbit recommended)
- **Graphics Adapter:** Onboard GFX, AGP or PCI-Express, minimum 1024 x 768, 16-bit color
- **Hard Disk Type:** E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster)
- **Hard Disk Space:** Minimum 10 GB free (depends on number of servers, cameras, rules, and logging settings)
- **Operating System:** Microsoft® Windows® Server 2008 R2 (64 bit), Microsoft® Windows® Server 2008 (32 or 64 bit), Microsoft® Windows® Server 2003 (32 or 64 bit)
- **Software:** Microsoft .NET 4.0 and Internet Information Services (IIS) 5.1 or newer.

Active Directory

OnSSI RC-E users are normally added from Active Directory, although users can also be added without Active Directory.

Active Directory is a distributed directory service included with several Windows Server operating systems; it identifies resources on a network in order for users or applications to access them.

If wishing to add users through the Active Directory service, a server with Active Directory installed, and acting as domain controller, must be available on your network.

Navigating the Built-in Help System

You are always able to freely navigate between the help system's contents. To do this, simply use the help window's three tabs: *Contents*, *Search*, and *Glossary,* or use the links inside the help topics.

- ***Contents Tab***: Lets you navigate the help system based on a tree structure. Many users will be familiar with this type of navigation from, for example, Windows Explorer. To go straight to the help system's *Contents* tab, click *Contents...* button in the Management Client's toolbar.

- ***Search Tab***: Lets you search for help topics containing particular terms of interest. For example, you can search for the term *zoom* and every help topic containing the term *zoom* will be listed in the search results. Clicking a help topic title in the search results list will open the required topic. To go straight to the help system's *Search* tab, click the *Search...* button in the Management Client's toolbar.

The actual content of each help topic is displayed in the right pane of the help window. Help topic texts may contain various types of links, notably so-called expanding drop-down links.

Clicking an expanding drop-down link will display detailed information. The detailed information will be displayed immediately below the link itself; the content on the page simply expands. Expanding drop-down links thus help save space.

To print a help topic, navigate to the required topic and click the browser's *Print* button.

Tip: When printing a selected help topic, the topic will be printed as you see it on your screen. Therefore, if a topic contains expanding drop-down links, click each required drop-down link to display the text in order for it to be included in your printout.

Installation and Removal

Installation Overview

If upgrading from a previous version of RC-E , make sure you read the upgrade information (see "Upgrade from Previous Version" on page 28).

If you plan to run **OnSSI Federated Architecture** (on page 173), make sure to read about important prerequisites.

Your RC-E installation process begins with the installation of the management server software.

- The **management server** is the center of your RC-E installation. It is typically installed on a dedicated server. See Management Server Installation (see "Install Management Server" on page 13).

Once the management server is installed, you are able to install key components required by the management server:

- The **recording server**, which is used for recording video feeds, and for communicating with cameras and other devices. The recording server is typically installed on one or more separate computers, rather than on the management server itself. See Install System Components (on page 17).
- The **management client**, also known as the **RC-E Manager**, which is used for configuration and day-to-day management of the system. The Management Client is typically installed on the system administrator's workstation or similar. See Management Client Installation (see "Management Client" on page 21).

Tip: Video device drivers (see "Manage and Remove Video Device Drivers" on page 190) are installed automatically during the initial installation of your RC-E system. However, new versions of the drivers are released from regularly and may be found on the OnSSI website.

As well on traditional servers, installation can also take place on virtualized servers.

Installing RC-E on Virtual Servers

As mentioned, it is possible to run all RC-E components on virtualized Windows® servers, such as - for example - VMware® and Microsoft Hyper-V®. Contact your IT department for more information.

Tip: Virtualization is often preferred to better utilize hardware resources. Normally, virtual servers running on the hardware host server do not load the virtual server to a great extent, and often not at the same time. However, RC-E recording servers record all cameras and streaming video. This puts high load on CPU, memory, network, and storage system. Thus when run on a virtual server, the normal gain of virtualization disappears to a large extent, since - in many cases - it will use all available resources.

If run in a virtual environment, it is important that the hardware host has the same amount of physical memory as allocated for the virtual servers and that the virtual server running the recording server is allocated enough CPU and memory - which it is not by default. Typically, the recording server needs 2-4 GB depending on configuration. Another bottleneck is network adapter allocation and hard disk performance. Consider allocating a physical network adapter on the host server of the virtual server running the recording server. This makes it easier to ensure that the network adapter is not overloaded with traffic to other virtual servers. If the network adapter is used for several virtual servers, the network traffic might result in the recording server not retrieving and recording the configured amount of images.

Install Management Server

If upgrading from a previous version of RC-E, make sure you read the upgrade information (see "Upgrade from Previous Version" on page 28).

If you plan to run **OnSSI Federated Architecture**, make sure to read about important prerequisites for running OnSSI Federated Architecture (see "OnSSI Federated Architecture Overview" on page 173).

Read the End User License Agreement on the Product License Sheet (enclosed with the software DVD) before installing any part of RC-E.

Your RC-E installation process begins with the installation of the RC-E management server software. The management server is the center of your OnSSI RC-E installation.

Prerequisites

- **Windows Installer 4.5 - only on Windows Server 2003**

  Before installing RC-E, it is important that you install Windows Installer 4.5. You can download the Windows Installer 4.5 (see http://www.microsoft.com/downloads - http://www.microsoft.com/downloads) from this link: http://www.microsoft.com/downloads **(see http://www.microsoft.com/downloads/ -** http://www.microsoft.com/downloads/**).**

- **SQL Server**

  The management server requires access to a relational database. Later in this installation process you must choose between using an existing SQL Server on the network (**Administrator rights** on the SQL Server are required) or setting up a SQL Server Express Edition (a lightweight, yet powerful, version of a full SQL server) on the management server computer itself.

  Whichever SQL solution you choose, make sure to have Microsoft .NET Framework 3.5 Service Pack 1 installed on the management server computer running the SQL Server Express Edition (even though Microsoft .NET Framework 4.0 is already installed) **or** the separate server running the existing SQL Server. See also System Requirements (on page 9).

  Which SQL Server type is right for our organization? The SQL Server Express Edition is easy to install and prepare for use, and will often suffice for systems with less than 500 cameras. However, if you plan to perform frequent/regular backups of your database, using an existing SQL Server on the network is recommended (**Administrator rights** on the SQL Server are required). For large installations, such as installations with 500 cameras or more, using an existing SQL Server on the network is always recommended.

- **Windows Server 2003 Fix**

  If you use Windows Server 2003 it is recommended to install this supported fix (see http://support.microsoft.com/kb/925336 - http://support.microsoft.com/kb/925336) for Windows Server 2003 before starting: http://support.microsoft.com/kb/925336 (see http://support.microsoft.com/kb/925336 - http://support.microsoft.com/kb/925336). Otherwise, the installation of your management server might fail due to Microsoft Windows Installer process having insufficient contiguous virtual memory to verify that the .msi package or the .msp package is correctly signed.

  The following steps assume that Ocularis Base has already been installed and licensed and the Base Component Installation web page is accessible from the machine where the RC-E Management Server is to be installed.

Installing

1. Shut down any OnSSI software running. If upgrading, it is highly recommended that you remove any previous versions of the management server before upgrading. Note, however, that you may not want to remove the management server database, as it contains your RC-E configuration.
2. From the Base Component install page, (http://<IP Address of Base machine>/OcularisService/InstallerWebsite/sysadmin.html), click the link for the RC-E Event Proxy and Recorder bundle.
3. Choose to 'Run' the executable.
4. When the download and security scan is complete, an 'Installation Wrapper' wizard screen appears. This wizard prompts you for a location to extract the installation files only. Verify or change the location (drive and directory) to place the installation file and click **Next**.
5. Once the files are extracted, you will see a screen with checkboxes to Install RC-E Event Proxy and RC-E Recorder.

   You may elect to install one, the other or both. In new and upgrade installations it is recommended to always install the Event Proxy. This installation will check the system for an existing proxy and, if found, will walk you through the process of uninstalling the old proxy and installing the new one. For the Recorder, this refers to the RC-E recorder components as a whole. For new installations, this box should be checked. For upgrade installations, see the Release Notes for special upgrade instructions.
6. Click **Finish**.
7. Follow the wizard prompts for the Event Proxy installation (if that checkbox was marked).
8. After the Event Proxy is installed, the RC-E Management Server files are extracted and a screen appears listing the steps involved in the installation:
9. Complete the steps outlined in the window.

   Tip: Depending on what is already installed on the computer which is going to act as management server, you may not need to complete all of the window's three steps. The step that currently requires your attention will be highlighted.

   Tip: When the management server software is installed, you are able to check the state of the management server by looking at the management server icon in the management server computer's notification area.

   See Management Server Service and Recording Server Service (on page 198) for more information.

Step 1: Internet Information Services

The RC-E Management Server Installation automatically detects if Internet Information Services (IIS) is already installed. If this step is not available, it is simply because IIS is already installed.

Internet Information Services includes a range of administrative features for managing web servers and web applications, and is required in order to run an OnSSI RC-E management server.

If installing on a server running Windows 2008 Server, IIS is automatically installed once you click the *Internet Information Services* step (should automatic installation fail, it is possible to do installation troubleshooting (on page 30)).

1. On Windows Server 2003, clicking the *Internet Information Services* step opens Windows' built-in *Windows Components* wizard:
2. In the wizard's *Components* list, select *Application Server***.**

Click *Details*... and select *Internet Information Services (IIS)*.

3. Click *Details*... and verify that all IIS subcomponents are selected. Click *OK* to return to the *Windows Components* wizard.
4. In the *Windows Components* wizard, click *Next* and follow the wizard.

Tip: It is a good idea to have your Windows installation DVD ready; it may be required during the process.

When IIS is installed, you will be returned to the *RC-E Management Server Installation* window for the next step of the installation.

Step 2: RC-E Management Server Database

Before completing this step, click the *View Microsoft SQL Server 2008 Express End-user License Agreement* link to read the license agreement for the software.

This step opens the *Database Setup* wizard, which will guide you through the process of preparing a database for use with the management server.

In the *Database Setup* wizard you will get the choice of using an existing SQL Server on the network or setting up a SQL Server Express Edition (a lightweight, yet powerful, version of a full SQL server) on the management server computer itself.

Follow the wizard's steps by clicking *Next*.

IMPORTANT: We recommend that you install the database on a dedicated hard disk drive that is not used for anything else but the database. Installing the database on its own drive will prevent low disk performance.

IMPORTANT: During the database preparation process, you will be asked whether you want to create a new database, use an existing database, or overwrite an existing database. For a new installation, you would typically select the default option *Create new database.* However, if you are installing the database as part of upgrading to a newer version of RC-E, and you want to use your existing database, make sure you select *Use existing database*.

When you have prepared the database, you will be returned to the *OnSSI RC-E Management Server Installation* window for the last step in the management server installation.

Step 3: RC-E Management Server

This step opens a wizard, which will guide you through the process of installing the management server software itself.

Follow the wizard's steps by clicking *Next*.

Tip: The wizard will ask you to specify the location of your temporary license (.lic) file. The system will verify your license file before you are able to continue. Therefore, have your license file ready.

On one of the wizard's steps, you will be asked to select between two installation options:

Typical (on page 16)

-or-

Custom (on page 16)

You may install the log server as part of the management server installation. But if required you can just as well install this on another server in your surveillance system:

- Installing the log server (see "Install Log Server (Custom)" on page 21) provides the necessary functionality for logging information from your RC-E installation.

Typical

If you select *Typical* installation, the wizard will install all the management server components at their default location and with other default settings. A Typical installation is recommended for most users.

Custom

If you select *Custom* installation, you get the option to select where to install each individual management server component. A *Custom* installation is recommended for advanced users.

Only relevant if selecting *Custom* installation:

On one of the wizard's steps you will be asked to select an IIS (Internet Information Services) web site for the Management Server service.

Select one of the listed web sites, and make sure the selected web site is started, then click *Next*. If the selected web site is not started, *Next* is disabled.

Tip: You may find that only a single IIS web site—the Default Web Site—is listed. In that case simply make sure that the web site is started, then click *Next*.

Towards the end of the wizard, in the *Service Log On Setup* window, you will be asked to select a user account under which the Management Server service will run:

You will be able to select either a:

- predefined Network Service account (see "Select a Predefined Account; Network Service" on page 16) (in which case the service will run whenever the computer acting as management server is running).

  - or -

- particular user account (see "Select a Particular User Account" on page 16) (in which case the service will use the specified user account to log in to the computer acting as management server).

Tip: If the computer acting as management server is a member of a domain, you should either select *Network Service*, or make sure that you specify a user account which belongs to the domain in question.

Select a Predefined Account; Network Service

1. Select *This predefined account*.
2. Select *Network Service*.
3. Click *OK*.

Select a Particular User Account

1. Select *This account*.
2. Click *Browse...*. This will open the *Select User* window.
3. In the *Select User* window, verify that the required domain is specified in the *From this location* field. If not, click *Locations...* to browse for the required domain.
4. In the *Enter the object names to select* box, type the required user name.

   Tip: Typing part of a name is often enough. Use the *Check Names* feature to verify that the name you have entered is recognized.
5. Click *OK*.

6. Specify the password for the user account in the *Password* field, and confirm the password in the *Confirm password* field.

   The password fields must not be empty; the password for the account must contain one or more characters and/or digits.

7. Click *OK*.

What's Next?

Upon installation of the management server software, the management server's built-in web page automatically opens in a browser. The web page lets you install key components required by the management server, among these:

- One or more **recording servers** (for recording video feeds and for communicating with cameras and other devices)
- A **Management Client** (for configuration and day-to-day management of the system)

Even though the web page opens automatically on the management server computer, you will in most cases want to install the key components on other computers than the management server itself. This is no problem since installation takes place through the web page, which can easily be accessed from other computers. See Install System Components (on page 17) for further information.

Install System Components

If upgrading from a previous version of RC-E, make sure you read the upgrade information (see "Upgrade from Previous Version" on page 28).

Installation of the following components is **not** covered in this section: log server (see "Install Log Server (Custom)" on page 21) and management server (see "Install Management Server" on page 13). See installation details for each.

Read the *End User License Agreement* on the Product License Sheet before installing any part of OnSSI RC-E.

IMPORTANT: As a prerequisite make sure of the following: During the installation process you will be asked to specify a user account under which the *Failover Server service* will run. For the failover solution to work, the failover server has to use the same user account as the recording server. Furthermore, the user account you specify must have access to your RC-E system with administrator rights. **Do the following to make sure of this...**

To verify whether the user account has administrator access to your OnSSI RC-E system, do the following:

1. In the Management Client's Site Navigation pane, expand Security and select *Roles*. In the overview pane's roles list, select the *Administrators* role.
2. In the properties pane's role settings list, verify that the required user is listed.
3. If the user is not listed, add the required user (see "Assign and Remove Users and Groups to/from Roles" on page 149) to the Administrators role by clicking *Add...* below the role settings list.

Part I—Downloading the Installer

The following describes the installation process. The process is more or less similar for the component types mentioned, so replace *the component* with *the OnSSI RC-E recording server*, *failover server* or *the Management Client*, depending on your needs.

1. On the computer on which you will install the component, shut down any OnSSI software running. If upgrading, it is highly recommended that you remove (see "Remove System Components" on page 27) any previous versions of the component before upgrading.
2. With a web browser, connect to the RC-E management server at the following address:

   http://[management server address]:[port]/installation/admin/

   where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

   This will open the management server's built-in web page. If not accessing the web page on the management server itself, log in with an account which has administrator rights on the management server.
3. On the web page find the relevant component's installer section, and then click the *English* link under the required recording server version (often, only one version will be available).

Depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking *Run* or similar (exact button text depends on your browser version).

Part II—Installing the Component

Select the relevant component for a description of the process (if required, repeat the process on other computers where the component should be installed):

Recording Servers

1. This will open the RC-E *Recording Server Setup* wizard, which will guide you through the installation.

   On the first step of the wizard, click *Next*.
2. Select installation method:

   Typical (see "Recording servers (Typical)" on page 18)

   - or -

   Custom (see "Recording servers (Custom)" on page 19)
3. Click *Install*.
4. On the last step of the wizard, click *Finish*. The recording server is now installed. The recording server has no user interface as such; it is accessed and managed through the Management Client.

Tip: When the recording server software is installed, you are able to check its state.

See Management Server Service and Recording Server Service (on page 198) for more information.

Recording servers (Typical)

The *Typical* option installs the RC-E recording server with default settings. A *Typical* installation is recommended for most users.

1. Specify recording server setup parameters (see "Specify Recording Server Setup Parameters" on page 21).
2. Click *Next*.

Recording servers (Custom)

The *Custom* option lets you select where to install the RC-E recording server components. A *Custom* installation is recommended for advanced users.

1. Select required installation folder, then click *Next*.
2. When asked which type of server to install, click the *Standard recording server* [...] icon. This lets you install a regular recording server.
3. Specify recording server setup parameters.
4. Click *Next*.
5. The wizard will ask you to select a user account under which the Recording Server service will run.

   You must select between:

   - a predefined system account (see "Select a Predefined System Account" on page 19)

     - or -

   - a particular user account (see "Select a Particular User Account" on page 20) (in which case the service will use the specified user account to log in to the computer acting as recording server).

     Tip: If the computer acting as recording server is a member of a domain, select the predefined account Local System or make sure you specify a user account which belongs to the domain in question.

     If using network drives, you should always specify a particular user account (which has access to the network drives in question), as the Recording Server service will not be able handle the network drives otherwise.
6. Click *Next*.
7. In some cases it can be advantageous to install more than one instance of the recording server on the same physical server (see "Multiple Recording Server Instances" on page 26). Specify the required number of instances (default is 1), then click *Next*.

   - Only relevant if installing more than one instance of the recording server on the same physical server: For each instance, specify the IP address to use for the instance in question.

     IMPORTANT: Note that the IP addresses you specify must be assigned to the physical server in question. Furthermore, even though your organization will not use IPv6 addresses, make sure to assign both IPv6 and IPv4 on the server as these are needed by the software.

     Tip: Provided enough IP addresses are assigned to the server, the fields will be pre-filled.
8. Click *Next*.

Select a Predefined System Account

1. Select *This predefined account*.
2. Select *Local System, Local Service*, or *Network Service* as applicable.
3. Click *OK***.**

Select a Particular User Account

1. Select *This account*.
2. Click *Browse...*. This will open the *Select User* window.
3. In the *Select User* window, verify that the required domain is specified in the *From this location* field. If not, click *Locations...* to browse for the required domain.
4. In the *Enter the object names to select* box, type the required user name.

   Tip: Typing part of a name is often enough. Use the *Check Names* feature to verify that the name you have entered is recognized.
5. Click *OK*.
6. Specify the password for the user account in the *Password* field, and confirm the password in the *Confirm password* field.

   The password must contain one or more characters and/or digits.
7. Click *OK*.

Failover Servers

1. This will open the RC-E *Recording Server Setup* wizard, which will guide you through the installation

   On the first step of the wizard, click *Next*.
2. Select installation method *Custom*.
3. Select required installation folder, and then click *Next*.
4. When asked which type of server to install, click the *Failover recording server for temporary* [...] icon.
5. Specify failover server setup parameters (see "Specify Recording Server Setup Parameters" on page 21).
6. Click *Next***.**
7. A failover server has two services:

   - A Failover Server service, which handles the processes of taking over from the regular recording server.
   - A Recording Server service, which enables the failover server to act as a recording server while the regular recording server is unavailable.

   The wizard will ask you to select a particular user account under which the services will run. Make your selection.

   See Select a Particular User Account... (see "Select a Particular User Account" on page 20) for how to select.

   For the failover solution to work, the user account you specify must have access to your RC-E system with administrator rights. If the computer acting as failover server is a member of a domain, make sure you specify a user account which belongs to the domain in question. If using network drives, always specify a user account which has access to the network drives in question.
8. Click *Install*.
9. On the last step of the wizard, click *Finish*. The failover server is now installed. The failover server has no user interface as such; it is accessed and managed through the Management Client.

Tip: When the failover server software is installed, you are able to check its state. See Management Server Service and Recording Server Service (on page 198) for more information.

Management Client

1. In the *Select installer language* drop down box, select language to use during the installation. In this example, we assume that you prefer English.
2. Next to appear is the RC-E *Management Client Setup* wizard, which will guide you through the installation process. On the first step of the wizard, click *Next***.**
3. Select required installation folder, then click *Next*.
4. Click *Install* to begin installation; wait while the required components are installed.
5. When ready, click *Finish***.**
6. To get an overview of the Management Client (see "Management Client Overview" on page 34), select *Launch RC-E Management Client.* This will start the Management Client (RC-E Manager) right away.

Specify Recording Server Setup Parameters

- **Name:** A name for the server in question. If required, you can later change the name through the RC-E Management Client.
- **RC-E management server:** The IP address (example: 123.123.123.123) or host name (example: ourserver) of the management server to which the server in question should be connected. If required, you can later change the management server IP address/host name as part of the basic administration on the Recording or Failover Server service.
- **MediaDB:** The path to the server in question's media database. The media database is the recording server's default storage area, i.e. the default location in which recordings from connected cameras are stored in individual camera databases. If required, you can later change the path, and/or add paths to more storage area locations, from the RC-E Management Client.

When should I choose a particular user account instead of a predefined? If using network drives you should always specify a particular user account (with access to the network drives in question). Otherwise the service in question is unable to handle the required network drives.

Install Log Server (Custom)

If upgrading from a previous version of RC-E , make sure you read the upgrade information (see "Upgrade from Previous Version" on page 28).

Installation of the following components are **not** covered in this section: recording servers, failover servers, Management Client (see "Install System Components" on page 17), and management server (see "Install Management Server" on page 13). See installation details for each.

Read the End User License Agreement on the Product License Sheet (enclosed with the software DVD) before installing any part of RC-E.

Normally, the log server is installed as part of the Management Server Installation (see "Install Management Server" on page 13), when installed with the *Typical* option. The following describes how to make a custom installation of the log server , when these are not installed as part of the *Typical* management server installation.

The log server can be installed either on the management server or on any other computer.

Make sure that user rights are set up correctly in the operating system. You can read about user rights in the operating system on Microsoft's web site_(http://technet.microsoft.com/en-us/library/cc794944(WS.10).aspx (see http://technet.microsoft.com/en-us/library/cc794944(WS.10).aspx - http://technet.microsoft.com/en-us/library/cc794944(WS.10).aspx).

Installing Log Server

The following describes the installation process (custom Installation).

1. On the computer on which you will install the log server, shut down any OnSSI software running. If upgrading, it is highly recommended that you remove (see "Remove System Components" on page 27) any previous versions of the server before upgrading.

2. Download the log server's installer from the management server's built-in web page at the address

   http://[management server address]:[port]/installation/admin/

   where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

   On the web page find the log servers' installer section, and then click the *English* link. Note that depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking *Run* or similar (exact button text depends on your browser version).

3. Run the installation file, either directly or from the location you saved it to. Follow the on-screen installation guide.

4. Verify/specify the required installation path and click *Next*.

5. Log Server:

   - Select the database to be used by the log server and click *Next*.
   - Select the web site on which you want to install and click *Next*.
   - Specify the URL address of the RC-E management server (example: *http://123.123.123.123*). If installing the server on the management server itself, simply specify localhost and click *Next*.

6. Specify a user account under which the log server's service will run. The specified user is automatically granted administrator rights in RC-E, see Specify the Rights of a Role (see "Specify Rights of a Role" on page 150).

   You must select between:

   - a predefined Network Service account (see "Select a Predefined Network Service Account" on page 23)(in which case the service will run whenever the computer acting as management server is running).

     -or -

   - a particular user account (see "Select a Particular User Account" on page 23) (in which case the service will use the specified user account to log in to the computer acting as recording server).

   When should I choose a particular user account instead of a predefined? If using network drives you should always specify a particular user account (with access to the network drives in question). Otherwise the service in question is unable to handle the required network drives.

7. Click *Install*. When installation is complete, click *Finish*.

Select a Predefined Network Service Account

1. The Network Service account is selected by default.
2. Click OK.

The Network Service account must be added as a Windows user on the relevant recording server computers in your surveillance system in order to retrieve status information from these recording servers.

Select a Particular User Account

1. Select *This account.*
2. Click *Browse...*. This will open the *Select User* window.
3. In the *Select User* window, verify that the required domain is specified in the *From this location* field. If not, click *Locations...* to browse for the required domain.
4. In the *Enter the object names to select* box, type the required user name.

   Tip: Typing part of a name is often enough. Use the *Check Names* feature to verify that the name you have entered is recognized.
5. Click *OK*.
6. Specify the password for the user account in the *Password* field, and confirm the password in the *Confirm password* field.

   The password must contain one or more characters and/or digits.
7. Click *OK*.

Important Port Numbers

OnSSI RC-E uses particular ports when communicating with other computers, cameras, etc.

What is a port? A port is a logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore it is sometimes, but not always, necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic which is used when viewing web pages.

When using RC-E, you must therefore make sure that certain ports are open for data traffic on your network.

The port numbers can be changed. Different port numbers may therefore be used in your organization. See Management Server Service and Recording Server Service (on page 198) for information about changing the recording server-related port numbers.

Tip: Consult the administrator of your organization's firewall if in doubt about how to open ports for traffic.

List of Ports Used by RC-E

Port 20 and 21 (inbound and outbound): Used by **recording servers** to listen for FTP information; some devices use FTP for sending event messages. FTP (File Transfer Protocol) is a standard for exchanging files across networks.

Port 25 (inbound and outbound): Used by **recording servers** to listen for SMTP information. Also, some devices use SMTP (e-mail) for sending event messages and /or for sending images to the surveillance system server via e-mail. SMTP (Simple Mail Transfer Protocol) is a standard for sending e-mail messages between servers.

Port 80 (inbound and outbound): While not directly used by RC-E , but by **management servers**, port 80 is typically used by the IIS (Internet Information Services) Default Web Site for running the RC-E Management Server service.

Port 554 (inbound and outbound): Used by **recording servers** for RTSP traffic in connection with H.264 video streaming.

Port 1024 and above (outbound only (except ports listed in the following)): Used by **recording servers** for HTTP traffic between cameras and servers.

Port 5210 (inbound and outbound): Used for communication between **recording servers** and **failover servers** when databases are merged after a failover server has been running.

Port 5432 (inbound and outbound): Used by **recording servers** to listen for TCP information; some devices use TCP for sending event messages.

Port 7563 (inbound and outbound): Used by **recording servers** and **Ocularis Client** for handling PTZ camera control commands and for communicating.

Port 8080 (inbound and outbound):Used for internal system communication**.**

Port 8844 (inbound and outbound): Used for communication between **failover servers**.

Port 9993 (inbound and outbound): Used for communication between **recording servers** and **management servers**.

Port 11000 (inbound and outbound): Used by **failover servers** for polling (i.e. regularly checking) the state of **recording servers**.

Port 65101(inbound and outbound): Used by **recording servers** for communication between recording servers and drivers (internally, used for example when SMTP events are received).

Any other port numbers you may have selected to use. Examples: If you have changed the IIS Default Web Site port from its default port number (80) to another port number, or if you have integrated RC-C servers into your RC-E system, in which case a port must be allocated for use by RC-C's Image Server service.

Multiple Management Servers (Clustering)

The RC-E management server can be installed on multiple servers within a cluster of servers. This ensures that RC-E has very little down-time: if a server in the cluster fails, another server in the cluster will automatically take over the failed server's job running the RC-E management server. The automatic process of switching over the RC-E server service to run on another server in the cluster only takes a very short time (up to 30 seconds).

Note that the allowed number of failovers is limited to two within a six hour period. If exceeded, Management Server services are not automatically started by the clustering service. The number of allowed failovers can be changed to better fit your needs. See Microsoft's homepage http://technet.microsoft.com/en-us/library/cc787861%28WS.10%29.aspx (see http://technet.microsoft.com/en-us/library/cc787861(WS.10).aspx - http://technet.microsoft.com/en-us/library/cc787861(WS.10).aspx) for details on how to do this.

Is clustering the same as federated architecture? No, clustering is not the same as federated architecture (see "OnSSI Federated Architecture Overview" on page 173). Clustering is a method to obtain failover support for a management server on a site. With clustering, it is only possible to have one active management server per surveillance setup, but other management servers may be set up to take over in case of failure. On the other hand, federated architecture, is a method to combine multiple independent corporate sites into one large setup, offering flexibility and unlimited possibilities.

Prerequisites for Installing OnSSI RC-E in a Cluster

- Two or more servers installed in a cluster.

  Tip: You can find information about failover clusters on Microsoft's web site.

  -Regarding clusters in Windows 2003, see Deploying Exchange Server 2003 in a Cluster (see http://technet.microsoft.com/en-us/library/bb123612(EXCHG.65).aspx - http://technet.microsoft.com/en-us/library/bb123612(EXCHG.65).aspx). http://technet.microsoft.com/en-us/library/bb123612(EXCHG.65).aspx)

  -Regarding clusters in Windows 2008, see Failover Clusters (see http://technet.microsoft.com/en-us/library/cc732488(WS.10).aspx - http://technet.microsoft.com/en-us/library/cc732488(WS.10).aspx).(http://technet.microsoft.com/en-us/library/cc732488(WS.10).aspx)

- **Either** an external SQL database installed **outside** the server cluster **or** an **internal** SQL service within the server cluster.

- A Microsoft® Windows® Server 2003/2008 Enterprise or Data Center edition.

Installing RC-E in a Cluster

The section is based on Windows 2008. So, if you are using Windows 2003, descriptions and illustrations might differ from what your see on your screen.

1. Install the RC-E management server and all its subcomponents on the first server in the cluster by following the procedures described in Install Management Server (on page 13).

   The management server must be installed with a specific user and not as a *Network Service***.** This requires that you use the *Custom* install option, see Install Management Server, step 3 (see "Install Management Server" on page 13), for details**.** Furthermore, the specific user must have access to the shared network drive and preferably a non-expiry password.

   The service channel and the IIS should both be installed normally with the exact same user, and *not* as cluster services.

2. After you have installed the management server and the Management Client on the first server in the cluster, open the Management Client, then from the *Tools* menu select *Registered Services...*

a) In the *Add/Remove Registered Services* window, select the *Log Service* in the list, then click *Edit...***.**

b) In the *Edit Registered Service* window, change the URL address of the log service to the URL address of the cluster.

c) Repeat steps a and b for all services listed in the *Add/Remove Registered Services* window.

d) In the *Add/Remove Registered Services* window, click *Network...*

e) In the *Network Configuration* window, change the URL address of the server to the URL address of the cluster. (This step only applies to the first server in the cluster.) Click *OK*.

3. Click *Close* in the *Add/Remove Registered Services* window, then exit the Management Client.

4. Stop the management server service (see "Management Server Service and Recording Server Service" on page 198) and the Internet Information Service (IIS). You can read about how to stop the IIS at Microsoft's homepage: http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx (see http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx - http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx).

5. Repeat steps 1-4 for all subsequent servers in the cluster, this time pointing to the existing SQL database, but for the **last** server in the cluster you install the management server on, do not stop the management server service.

The management server service must be configured as a generic service in the failover cluster in order to take effect:

1. On the last server you have installed the management server on, open Windows' *Failover Cluster Management*, found under *Administrative Tools* in the *Start* menu.
2. In the *Failover Cluster Management* window, expand your cluster, right-click *Services and Applications*, then select *Configure a Service or Application...*
3. On the first page of the *High Availability* wizard click *Next*, then on the second page of the wizard select *Generic Service* in the list, and click *Next*.
4. Do not specify anything on the third page of the wizard, click *Next*.
5. Select the *OnSSI RC-E management server* service from the list, then click *Next*.
6. Specify the name (host name of the cluster), that clients will use when accessing the service, then click *Next***.**
7. No storage is required for the service, click *Next*.
8. No registry settings should be replicated, click *Next***.**
9. Verify that the cluster service is configured according to your needs, then click *Next***.**
10. The RC-E management server has now been configured as a generic service in the failover cluster. Click *Finish* to exit the wizard.

Upgrading RC-E in a Cluster

Prerequisite

Make sure to have a backup of the database in question before updating the cluster.

How To Update...

1. Stop Management Server services (see "Management Server Service and Recording Server Service" on page 198) on all management servers in the cluster.
2. Uninstall the management server on all servers in the cluster. See Remove System Components (on page 27).
3. Use the procedure for installing multiple management servers in a cluster as described in Installing RC-E in a Cluster (on page 25).

IMPORTANT: When installing, make sure to reuse the existing SQL configuration database (which will automatically be upgraded from the old existing database version to the new one).

Multiple Recording Server Instances

It is only recommended to install multiple instances of the Recording Server service on the same server under the following conditions.

If you:

- are upgrading from RC-E 4.1 or older

—and—

- are already running more 32-bit Recording Server service instances on the same server.

Since it is not possible to move devices/cameras from one recording server to another, setups running more than one 32-bit Recording Server service instances on the same server, will need to maintain this structure.

For all other setups, the newer 64-bit recording server eliminates the need for running more 32-bit instances on the same server.

Installing Multiple Recording Server Instances

During the recording server installation (see "Install System Components" on page 17), you simply select the required number of instances. A maximum of 99 recording server instances is allowed on a single server.

Using multiple recording server instances does not require additional licenses.

In the Management Client, each recording server instance will be displayed separately, allowing you to configure each instance separately.

When managing the Recording Server service (see "Management Server Service and Recording Server Service" on page 198) by right-clicking its icon in the notification area on the server itself, you can:

- Stop and start each instance individually
- View status messages for each instance individually, grouped on tabs.

Remove System Components

If you are not an RC-E system administrator, do not attempt to remove the management software.

The following procedure describes standard system component removal in recent Windows versions; the procedure may be slightly different in older Windows versions:

1. In Windows' *Start* menu, select *Control Panel*, and then...
   - If using *Category* view, find the *Programs* category, and click *Uninstall* a program.
   - If using *Small icons* or *Large icons* view, select *Programs and Features*.
2. In the list of currently installed programs, right-click the required program or service, select *Uninstall*, and follow the removal instructions.

Removing Management Server

OnSSI RC-E management servers are most likely installed on a dedicated server.

To remove, follow the general removal procedure (see "Remove System Components" on page 27).

Removing Download Manager and Log Server

The **Download Manager** and **log server,** which are all installed on the management server, are removed separately from the management server software.

To remove, follow the general removal procedure (see "Remove System Components" on page 27).

Removing Management Client

OnSSI RC-E Management Client are all removed at the computer on which the program or service is installed.

To remove, follow the general removal procedure (see "Remove System Components" on page 27).

Removing Recording Server

To remove an **RC-E recording server**, use the following procedure on the computer on which the recording server is installed:

What happens to the recording server's recordings? During the removal process, you will be asked whether you want to keep the recording server's recordings.

1. Stop the recording server service by right-clicking the recording server icon in the computer's notification area (also known as the *system tray*), then selecting *Stop Recording Server Service*.

2. To remove, follow the general removal procedure (see "Remove System Components" on page 27). Right-click the *RC-E Recording Server* in step 2 of the process.

Upgrade from Previous Version

This information is only relevant if you are upgrading a previous installation of RC-E.

IMPORTANT: RC-E no longer supports Microsoft® Windows® XP. See System Requirements (on page 9).

The process of upgrading RC-E involves removing all of its components **except** the Database Server. The Database Server is one of the management server's components, it contains the entire system configuration (recording server configurations, camera configurations, rules, etc.). As long as you do not remove the Database Server, you will not need to reconfigure your surveillance system configuration in any way (although you may of course want to configure some of the new features in the new version).

Backward compatibility with recording servers from RC-E versions older than 3.0 is limited. You can still access recordings on such older recording servers; but in order for you to be able to change their configuration, they must be of version 3.0 or later. It is thus highly recommended that you upgrade all recording servers in your RC-E system.

When doing an update which includes updating your recording servers, you automatically update your Video Device Drivers as well. In this case, after restarting your system, it might take several minutes for your hardware devices to make contact with the new Video Device Drivers, so have patience. This is due to several internal checks being performed on the newly installed drivers.

Prerequisites

- Have your **temporary license (.lic) file** ready. The license file will change when your SLC changes, so you are likely to have received a new license file when purchasing the new version. When you install the management server, the wizard will ask you to specify the location of your license (.lic) file, which the system will verify before you will be able to continue.

  If you do not have your license file, contact your OnSSI vendor.

- Have your **new RC-E version** ready. If you have not purchased the software on a DVD, you can download it from www.onssi.com (http://www.onssi.com). Note that although you can download any version, you will only be able to install a version for which your license file is valid.

- The management server stores your RC-E system's configuration in a database. The system configuration database can be stored in two different ways: 1) In a SQL Server Express Edition database on the management server itself, or 2) in a database on an existing SQL Server on your network. If using 2), **Administrator rights on the SQL Server** are required whenever you need to create, move or upgrade the management server's system configuration database on the SQL Server. Once you are done creating, moving or updating, being database owner of the management server's system configuration database on the SQL Server will suffice.

Upgrading the Management Server

The management server has several components. This describes removing old components—except the Database Server—and installing the new ones:

1. First remove the management server itself. See Remove System Components (on page 27).
2. Next, remove the RC-E Windows components.
3. If the RC-E Management Client is installed on the management server itself, remove the Management Client too. See Remove System Components (on page 27).
4. Run the installation for the new version of RC-E. After a short while, the installation window will open. Out of the three installation steps for the management server, you will be asked to address step 3 (OnSSI RC-E management server).
5. Click the installation window's step 3, and complete the RC-E management server installation. During this process you will be asked to specify the path to your license (.lic) file.
6. When the management server is installed, the management server's web page will appear in a browser. If you want to install the Management Client software on the management server itself, you can do it from the management server's web page.

Upgrading Recording Servers

Once the new management server is installed, you can remove the old recording server version, and install the new one:

What happens to the recording server's recordings? During the removal process, you will be asked whether you want to keep the recording server's recordings.

1. See Remove System Components (on page 27) for how to remove a recording server.
2. When the recording server has been removed, open a browser and connect to the management server's web page at the following address:

   http://[management server address]:[port]/installation/admin/

   where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

   If not accessing the web page on the management server itself, log in with an account which has administrator rights on the management server.
3. From the web page, install the new version of the recording server software.
4. Repeat for each recording server on your RC-E system.

When updating your recording servers, you automatically update your Video Device Drivers as well. After restarting your recording servers, it might take several minutes for your hardware devices to make contact with the new Video

Device Drivers, so have patience. This is due to several internal checks being performed on the newly installed drivers.

Upgrading a Management Client

If the Management Client is installed on separate computers, such as the surveillance system administrator's workstation or similar, you should now remove the old version and install the new one:

1. See Remove System Components (on page 27) for details on removing a Management Client.
2. When the Management Client has been removed, open a browser and connect to the management server's web page at the following address:

   http:///[management server address]:[port]/installation/admin/

   where [management server address] is the IP address or host name of the management server, and [port] is the port number which IIS has been set up to use on the management server.

   If not accessing the web page on the management server itself, log in with an account which has administrator rights on the management server.
3. From the web page, install the new version of the Management Client.

Upgrading Video Device Drivers

Before upgrading Video Device Drivers, you must remove old Video Device Drives.

For information on how to remove/upgrade/install Video Device Drivers, see Manage and Remove Video Device Drivers (on page 190).

Installation Troubleshooting

The following issues may occasionally occur during or upon installation of the RC-E management server or recording servers. For each issue, one or more solutions are available.

Issue: Automatic IIS Installation for Mgmt.

If installing the management server on a server running Windows 2008 Server, Internet Information Services (IIS) is under normal circumstances automatically installed.

- For the management server, this happens when you click the Internet Information Services step in the RC-E Management Server Installation window.

If the automatic installation fails, you can install IIS manually.

Solution: Install IIS Manually

1. If automatic IIS installation fails, you will see an error message asking you to install IIS manually. In the error message box, click *Install IIS Manually*.
2. You will now see the *Server Manager* window. In the left side of the window, select *Roles*, then the *Roles Summary*.
3. Now select *Add Roles* to start a wizard.

4. In the wizard, click *Next*, select *Web Server (IIS)*, and follow the wizard's steps.
5. When you reach the wizard's *Select Role Services* step, you will see that some role services are selected by default. However, you should select some additional role services:
    - Under *Security*, select *Basic Authentication* and *Windows authentication*.
    - Under *Management Tools*, select *IIS 6 Management Console*, expand it, and select *IIS 6 Metabase Compatibility*, *IIS 6 WMI Compatibility*, *IIS 6 Scripting Tools*, and *IIS 6 Management Console*.
6. Complete the wizard by following the remaining steps.

Issue: Recording Server Startup Fails due to Port Conflict

This is an issue if either the Simple Mail Transfer Protocol **(**SMTP) Service or an existing installation of RC-C is running.

Both use port 25. If port 25 is already in use, it may not be possible to start the RC-E Recording Server service. It is important that port number 25 is available for the recording server's SMTP service since many cameras are only capable of communicating via this port.

SMTP Service: Verification and Solutions

To verify whether SMTP Service is installed, do the following:

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Add or Remove Programs*.
3. In the left side of the *Add or Remove Programs* window, click *Add/Remove Windows Components*.
4. In the *Windows Components* wizard, select the *Internet Information Services (IIS)* item, and click *Details...*.
5. In the *Internet Information Services (IIS)* window, verify whether the *SMTP Service* check box is selected. If it is, SMTP Service is installed.

If SMTP Service is installed, select one of the following solutions:

Solution 1: Disable SMTP Service, or set it to manual startup

This solution lets you start the recording server without having to stop the SMTP Service every time:

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Administrative Tools*.
3. In the *Administrative Tools* window, double-click *Services*.
4. In the *Services* window, double-click the *Simple Mail Transfer Protocol (SMTP)* item.
5. In the *SMTP Properties* window, click *Stop*, then set *Startup type* to either *Manual* or *Disabled*.

    Tip: When set to *Manual*, the SMTP Service can be started manually from the *Services* window, or from a command prompt using the command *net start SMTPSVC*.
6. Click *OK*.

Solution 2: Remove SMTP Service

Note that removing the SMTP Service may affect other applications using the SMTP Service.

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Add or Remove Programs*.
3. In the left side of the *Add or Remove Programs* window, click *Add/Remove Windows Components*.
4. In the *Windows Components* wizard, select the *Internet Information Services (IIS)* item, and click Details....
5. In the *Internet Information Services (IIS)* window, clear the *SMTP Service* check box.
6. Click *OK, Next*, and *Finish*.

OnSSI RC-C: Verification and Solutions

To verify whether RC-C is installed, do the following:

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Add or Remove Programs*.
3. In the *Add or Remove Programs* window, verify whether RC-C appears in the list. If it does, RC-C is installed.

If RC-C is installed, select one of the following solutions:

Solution 1: Remove RC-C

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Add or Remove Programs*.
3. In the *Add or Remove Programs* window, select RC-C, click *Uninstall*/*Change*, and then *OK*.

Solution 2: Set RC-C Services to manual startup

This solution lets you start the recording server without having to stop the RC-C Services every time:

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Administrative Tools*.
3. In the *Administrative Tools* window, double-click *Services*.
4. In the *Services* window, repeat steps a-c for these items: *OnSSI ImageImportService, OnSSI ImageServer, OnSSI LogCheckService, OnSSI Recording Server.*
5. Double-click the item.
6. In the *<item> Properties* window, click *Stop*, then set *Startup type* to *Manual*.
7. Click *Close*.

Tip: With the startup type *Manual*, you can start and stop the RC-C Services from a command file:

To start the RC-C Services from a command file, create a file named e.g. *startx.cmd* with the following content:

```
net start "OnSSI ImageImportService"
net start "OnSSI ImageServer"
net start "OnSSI LogCheckService"
net start "RecordingServer"
```

To stop the RC-C Services from a command file create a file named e.g. *stopx.cmd* with the following content:

```
net stop "OnSSI ImageImportService"
net stop "OnSSI ImageServer"
net stop "OnSSI LogCheckService"
net stop "RecordingServer"
```

Issue: Changes to SQL Server Location Prevents Database Access

This is an issue if using an MS SQL Server database as the RC-E management server database: If the location of the SQL Server is changed, for example by changing the host name of the computer running the SQL Server, access to the database will be lost.

Solution: Run Management Server Database Installation Step Again

See Management Server Installation (see "Install Management Server" on page 13). When running the database installation, you will - during the database preparation process - be asked whether you want to create a new database, use an existing database, or overwrite an existing database: Pointing to the new location of the SQL Server, select to use an existing database. This will update the SQL connection string used by the management server, and it will again be possible to access the database.

Issue: Insufficient Continuous Virtual Memory Fails Installation

The following is only relevant if you use **Windows Server 2003.**

If you try to install a large Windows Installer package or patch package in Windows Server 2003, this problem might occur if the Windows Installer process has insufficient continuous virtual memory to verify that the .msi package or the .msp package is correctly signed.

Solution: A supported fix (see http://support.microsoft.com/kb/925336 - http://support.microsoft.com/kb/925336) **is available for Windows Server 2003.** See http://support.microsoft.com/kb/925336 (see http://support.microsoft.com/kb/925336 - http://support.microsoft.com/kb/925336).

Issue: Multi-domain Environments; One-way Trusts not Working

See Multi-domain Environments, One-way Trust.

Management Client (RC-E Manager)

Management Client (RC-E Manager) Overview

The Management Client, also known as the RC-E Manager, is the feature-rich administration client used for configuration and day-to-day administration of your RC-E system. The Management Client software is typically installed (see "Install System Components" on page 17) on the surveillance system administrator's workstation or similar. The term 'Management Client' is a generic name used for the 'RC-E Manager'.

Management Client's Elements

The Management Client window is divided into a number of panes. The number of panes will change depending on your task:

The following illustrations outline the Management Client window's default layout; the window layout can be customized (see "Customize the Management Client's Layout" on page 41), and may therefore be different on your computer.

- When working with recording servers and devices (cameras, inputs, outputs), the Management Client window contains a menu bar (on page 35) and four panes (see "Panes Overview" on page 36):
- When working with rules, time and notification profiles, users, roles, etc., the Management Client window typically contains a menu bar (on page 35) and three panes (see "Panes Overview" on page 36):
- When viewing logs, the Management Client window typically contains only the menu bar, (see "Menu Bar" on page 35) the Site Navigation and Federated Sites Hierarchy Pane (see "Site Navigation Pane and Federated Hierarchy Pane" on page 34) and an overview area (marked in gray):

Site Navigation Pane and Federated Hierarchy Pane

The Management Client is the feature-rich administration client used for configuration and day-to-day administration of your RC-E system. The Management Client software is typically installed on the surveillance system administrator's workstation or similar. The term 'Management Client' is a generic name used for the 'RC-E Manager'.

Site Navigation Pane

This is your main navigation element in the Management Client. Name, settings and configurations of the site you are logged into are reflected (see "Manage OnSSI Federated Architecture" on page 177) here (site-name is visible at the top of the pane). The Management Client's features are grouped into the following categories:

- ***Basics***: General information, for example about licenses in your RC-E system
- ***Servers***: Management of recording servers and failover servers (spare recording servers) connected to your RC-E system
- ***Devices***: Management of cameras, microphones, speakers, input, and output
- ***Client***: Management of view groups

- ***Rules and Events:*** Management of rules, time profiles, notification profiles, events and events settings.
- ***Security***: Management of users, groups, and roles
- ***System Dashboard***: System reporting functionality and overview of recording servers' databases and archives
- ***Server Logs***: Access to the various logs of your RC-E system

Tip: Right-clicking items in the Site Navigation pane gives you quick access to management features.

Federated Site Hierarchy Pane

Your navigation element dedicated to displaying OnSSI Federated Architecture (see "OnSSI Federated Architecture Overview" on page 173) sites and their parent/child links.

The parent server you are logged in to, a.k.a your home site, will always be at top, and adopting its point of view, you can view all its linked children and downwards in the parent/child hierarchy.

What if I only have one server and don't run OnSSI Federated Architecture? Your user interface looks the same, but you will only see the one server in your setup.

Menu Bar

The Management Client's menu bar features the following menus (see "Management Client Menu Overview" on page 40):

File Menu, *Edit* Menu, *View* Menu, *Action* Menu, *Tools* Menu and *Help* Menu.

Toolbar

The Management Client's toolbar features the following options:

Save: Save changes to your settings.

Undo: Undo your latest change.

Help...: Access a help topic relevant to your task

Contents...: Access the help system's table of contents.

Search...: Access the help system's search feature.

Tip: Read more about the Management Client's built-in help system in Use the Built-in Help System (see "Navigating the Built-in Help System" on page 11).

Memory Indicator

The memory indicator located in the lower left corner of the Management Client states how much memory is available for working with the Management Client.

When you expand items in the Site Navigation pane the Management Client uses memory to treat data stored in the individual items. Expanded items keep processing even when you expand other items in the Site Navigation pane, thus letting you access already-expanded items faster.

When available memory drops to 300 MB the memory indicator numbers turn red.

When the memory indicator drops to 0 MB, meaning there is no more memory available for the Management Client, you cannot expand any more items.

To free up memory, refresh the Management Client: Click *OK* to exit the dialog, then press F5 on your keyboard or select *Refresh* from the *Action* menu.

Panes Overview

The Management Client window may contain up to four panes.

1. Site Navigation Pane and Federated Sites Hierarchy Pane (see "Site Navigation Pane and Federated Hierarchy Pane" on page 34)
2. Overview Pane (on page 36)
3. Properties Pane (on page 36)
4. Preview Pane (on page 36)

The illustration outlines the Management Client window's default layout; the window layout can be customized (see "Customize the Management Client's Layout" on page 41), and may therefore be different on your computer.

Menu and Tool Bars

Provide quick access to often-used features.

Overview Pane

Provides an overview of the item you have selected in the navigation pane, typically in the form of a detailed list.

Selecting a particular item in the overview pane will typically display the item's properties in the properties pane. Right-clicking items in the overview pane gives you access to management features.

Preview Pane

Displays preview images from selected cameras or state information from selected microphones, speakers, inputs and outputs. The example to the left shows a camera preview image with information about the resolution and data rate of the camera's live stream.

Tip: By default, information shown with camera preview images will concern live streams (shown in green text). If you want recording stream information instead (shown in red text), select *View > Show Recording Streams* from the Management Client's menu.

You will see the preview pane when you deal with recording servers and devices. You can toggle the preview pane on and off in the *View* menu. To resize the preview pane, drag its borders. The larger the preview pane, the larger preview images and state information will appear.

Tip: Performance can be affected if the preview pane displays preview images from many cameras at a high frame rate. To control the number of preview images, and their frame rate, select *Options > General* from the *Tools* menu.

Properties Pane

Displays properties of the item selected in the overview pane. In many cases, properties are displayed across a number of tabs:

Site Navigation Pane and Federated Hierarchy Pane

The Management Client is the feature-rich administration client used for configuration and day-to-day administration of your RC-E system. The Management Client software is typically installed on the surveillance system administrator's workstation or similar. The term 'Management Client' is a generic name used for the 'RC-E Manager'.

Site Navigation Pane

This is your main navigation element in the Management Client. Name, settings and configurations of the site you are logged into are reflected (see "Manage OnSSI Federated Architecture" on page 177) here (site-name is visible at the top of the pane). The Management Client's features are grouped into the following categories:

- ***Basics***: General information, for example about licenses in your RC-E system
- ***Servers***: Management of recording servers and failover servers (spare recording servers) connected to your RC-E system
- ***Devices***: Management of cameras, microphones, speakers, input, and output
- ***Client***: Management of view groups
- ***Rules and Events:*** Management of rules, time profiles, notification profiles, events and events settings.
- ***Security***: Management of users, groups, and roles
- ***System Dashboard***: System reporting functionality and overview of recording servers' databases and archives
- ***Server Logs***: Access to the various logs of your RC-E system

Tip: Right-clicking items in the Site Navigation pane gives you quick access to management features.

Federated Site Hierarchy Pane

Your navigation element dedicated to displaying OnSSI Federated Architecture (see "OnSSI Federated Architecture Overview" on page 173) sites and their parent/child links.

The parent server you are logged in to, a.k.a your home site, will always be at top, and adopting its point of view, you can view all its linked children and downwards in the parent/child hierarchy.

What if I only have one server and don't run OnSSI Federated Architecture? Your user interface looks the same, but you will only see the one server in your setup.

Basics

Get Started

The tasks typically involved in setting up an RC-E system are listed below.

Note that although information is presented as a checklist, a completed checklist does not in itself guarantee that the RC-E system will match the exact requirements of your organization. To make the system match the needs of your organization, it is highly recommended that you monitor and adjust the system once it is running.

For example, it is often a good idea to spend time on testing and adjusting the motion detection sensitivity settings of individual cameras under different physical conditions (day/night, windy calm weather, etc.) once the system is

running. The setup of rules, which determine most of the actions performed by the RC-E system (including when to record video), is another example of configuration which to a very large extent depends on your organization's needs.

The following steps should be completed after the installation and licensing of Ocularis Base.

- Install the various components of your RC-E system. See Installation Overview (on page 12).
- Log in to the Management Client. See Log in to the Management Client (on page 39).
- Authorize use of your RC-E system's recording servers. See Manage Recording Servers (on page 60).

Why must I authorize recording servers? By authorizing recording servers before they can be used, surveillance system administrators have full control over which recording servers are able to send information to their RC-E management server.

- Detect the hardware devices (i.e. cameras and video encoders) which should be added to each recording server. See the wizard Add Hardware (see "Add Hardware (Cameras, etc.)" on page 49).

What is the Add Hardware wizard?*Add Hardware* helps you detect IP hardware devices, such as cameras and video encoders, on your network and add them to your RC-E system. The wizard offers you two ways of detecting and adding hardware devices: With *automatic hardware detection*, RC-E automatically scans for available hardware within one or more specified IP address ranges. With *assisted hardware detection*, you manually specify the IP address of each required device. Both options offer the possibility of automatically detecting the correct hardware drivers.

- Verify that each recording server's storage areas will meet your needs. See About Storage and Archiving (on page 56).

What is a storage area? A storage area is a directory in which the databases containing recordings from the cameras connected to the recording server are stored— each individual camera database by default has a maximum size of 5 GB. A default storage area is automatically created for each recording server when the recording server is installed on the system. Connected cameras' databases are stored in the recording server's default storage area unless you specifically define that another storage area should be used for storing the databases of particular cameras. If required, a wizard lets you add further storage areas (on the recording server computer itself, or at another location, for example on a network drive), edit which storage area should be the default area, etc.

- Verify that each recording server's archiving settings will meet your needs. See About Storage and Archiving (on page 56).

What is archiving? Archiving is the automatic transfer of recordings from a camera's default database to another location. This way, the amount of recordings you are able to store will not be limited by the size of the camera's default database. Archiving also makes it possible to back up your recordings on backup media of your choice. Archiving is configured on a per-recording server basis. Once you have configured the archiving settings for a recording server (where to store archives, how often to transfer recordings to the archives, etc.), you can enable archiving for individual cameras. When archiving is enabled for a camera, the contents of the camera's database will automatically be moved to an archive at regular intervals.

- Configure any required failover servers. A failover server is a spare recording server which can take over if a regular recording server becomes unavailable. See About Failover Servers (see "Manage Failover Servers" on page 192).
- Configure each recording server's individual cameras. See Manage Cameras (on page 75).

Tip: You are able to group cameras, and configure common properties for all cameras within a group in one step.

Tip: Motion detection, a vital setting on most IP surveillance systems, is enabled by default. However, you may want to fine-tune motion detection settings, or disable motion detection for particular cameras.

Enable and configure microphones— if any. See Manage Microphones (on page 85).

- Enable and configure speakers— if any. See Manage Speakers (on page 87).
- Enable and configure input— if any. See Manage Inputs (see "Manage Input" on page 88).
- Enable and configure output— if any. See Manage Outputs (see "Manage Output" on page 91).

- Create rules. See Manage Rules (on page 133).

What is a rule? Rules are a central element in RC-E. The behavior of an RC-E system is to a very large extent determined by rules. Rules determine highly important settings, such as when cameras should record, when PTZ (Pan/Tilt/Zoom) cameras should patrol, when notifications should be sent, etc.

Tip: When creating rules, you may also want to use time profiles (see "Manage Time Profiles" on page 138) (for quickly making rules apply within or outside predefined periods of time) or notification profiles (see "Manage Notification Profiles" on page 141) (for quickly making rules send pre-configured e-mails— with video clips, if required— to selected recipients).

- Add roles. See About Roles (on page 145).

What is a role? Roles determine which RC-E features users and groups are able to use. In other words, roles determine rights.

- Add users and/or groups of users. See About Users and Groups (see "Manage Users and Groups" on page 145).

Tip: If you have a server with Active Directory installed, and acting as domain controller on your network, RC-E lets you quickly add users and/or groups from Active Directory.

- Activate licenses. See About Licensing (see "Manage Licenses" on page 45).

Why must licenses be activated? When installing the system, you used a single temporary license. The temporary license is only valid for a certain number of days. After this initial period ends, all recording servers and cameras on your system will require activation of their individual licenses. You must therefore activate your licenses before the initial period ends, since all recording servers and cameras for which no licenses have been activated will otherwise stop sending data to the surveillance system.

- Use the Download Manager to make additional components available to users—if required. See Use the Download Manager.

What is the Download Manager? An application which lets surveillance system administrators manage which system-related components (e.g. particular language versions of clients) surveillance system users will be able to access from a targeted web page generated by the management server.

Log in to the Management Client

Access to the RC-E Management Client requires certain user rights. Consult your surveillance system administrator if in doubt.

1. Click the RC-E Management Client desktop icon or—in Windows' *Start* menu—select *All Programs* > RC-E > *Management Client*. This will make the login window appear:

2. The login window's *Server type* field will in many cases appear dimmed and pre-filled with the required information. If not, select RC-E.

3. In the *Server address* field, type the IP address or host name of the computer running the RC-E management server.

   Tip: If you have logged in before, you can select previously used server IP addresses or host names from the list.

4. By default, you will log in to the management server with your active Windows account. This means that if you are currently logged in as, for example, *JohnSmith*, you will by default log in to the management server as *JohnSmith* as well.

   o If you wish to log in to the management server with your active Windows account (this is the default login option), select *Windows Authentication (current user)* in the *Authentication* field.

- If you wish to log in to the management server with a different Windows account, select *Windows Authentication* in the *Authentication* field, then type the required user name and password in the *User name* and *Password* fields respectively.

Tip: If you have logged in with *Windows Authentication* before, you can select previously entered user names from the list.

Tip: When using *Windows Authentication*, you have the option of selecting *Remember password*, in which case you will not have to type the password at subsequent logins.

5. Click *Connect* to open Management Client.

Management Client Menu Overview

Action Menu Items

(Depending on context)

- ***Refresh*** is always available and reloads the requested information from the management server.
- ***Expand*** (or *Collapse*) is available when working with *Federated architecture*, *Servers*, *Devices, Client, Rules* and *Events* and *System Dashboard*.
- A number of context specific items.

Be aware of the following when working with the *Action* menu concerning OnSSI Federated Architecture (see "OnSSI Federated Architecture Overview" on page 173): To be able to delete a site without being connected to it, **right-clicking a site does not select it, but offers a context menu**. Because of this, some context menu items may be disabled if you are not connected to the site and some are only available on the home-site, i.e. the site you are logged in to. For more details see Manage OnSSI Federated Architecture (see "OnSSI Federated Architecture Overview" on page 173).

Edit Menu Items

- ***Undo*** lets you cancel your latest action.

  Tip: As an alternative to selecting *Edit* > *Undo*, press CTRL+Z on your keyboard.

File Menu Items

- ***Save***: Lets you save your current configuration.

  Tip: As an alternative to selecting File > Save, press CTRL+S on your keyboard.

- ***Logoff***...: Lets you log out of the Management Client, and log in with another user account if necessary.
- ***Exit*****:** Lets you close down and exit the Management Client.

Help Menu Items

- ***Help***... lets you access a help topic relevant to your task.
- ***Contents***... lets you access the help system's table of contents.

- ***Search***... lets you access the help system's search feature.
- ***About***... opens a dialog displaying information about the version of your Management Client.

Tools Menu Items

- ***Registered Services***... lets you add trusted servers. See Manage Trusted Servers for details.
- ***RC-C Servers***... lets you add RC-C servers specifically. See Manage RC-C Servers (on page 162) for details.
- ***Effective Roles.***.. lets you view all roles of a selected user or group (see "Manage Users and Groups" on page 145). For more information, see Manage Roles (on page 147).
- ***Options.***.. opens the Options dialog (see "Options" on page 168), which lets you define and edit several global RC-E settings.

View Menu Items

(Depending on context)

- ***Reset Application Layout****:* Lets you reset the layout of the different panes in the Management Client to their default settings. See Customize the Management Client's Layout (see "Customize the Management Client's Layout" on page 41)t for details.
- ***Preview Window****:* Lets you toggle the preview pane (see "Panes Overview" on page 36) on and off when working with recording servers and devices.

  Tip: If the preview pane displays images from many cameras at a high frame rate, it may slow down performance. To specify the number of preview images you want in your preview pane, as well as their frame rate, select *Options > General* from the *Tools* menu.

- ***Show Recording Streams***: By default, the information shown with preview images in the preview pane will concern cameras' live streams (shown in **green** text). If you want information about recording streams instead, select *Show Recording Streams*. Recording stream information will be shown in **red** text.
- ***Federated Site Hierarchy***: By default, the is enabled, and this command lets you toggle it on and off.
- ***Site Navigation:*** By default, the Site Navigation pane (see "Panes Overview" on page 36) is enabled, and this command lets you toggle it on and off.

Customize the Management Client's Layout

You can rearrange panes in the Management Client, and thus customize its look to suit your needs. If you rearrange the panes, you can always reset the entire layout to the Management Client's default layout.

Resizing Panes

You can resize panes by dragging the borders of the panes:

1. Place your mouse pointer over a border.
2. When the pointer becomes a double-headed arrow, drag the border in the required direction.

The size of the content inside the panes stays the same regardless of the size of the panes, with one exception: the larger the preview pane is, the larger preview images and state information will appear.

Moving Panes

You can move a pane to a different position either as a floating pane or to a docked position, by clicking on a pane's title bar and dragging it with the mouse.

The position and whether the pane becomes a floating pane or docked depend on where you release the mouse button. See the following topics for more information.

The Management Client offers some layout elements that help you control the new position of the pane.

The layout elements are available when you drag a pane.

For more information about how you use the layout elements when moving panes see these topics:

Floating Panes

To move a pane to a floating pane, drag the pane to its new position *without* using one of the layout elements.

Moving a Pane to a Docked Outer Position

If you move a pane to a docked outer position, it fills the area with a horizontal or vertical split that goes from top to bottom or left to right.

1. Drag the pane to one of the outer layout elements.

   Tip: Before you release the mouse, the pane's new position is indicated by a gray area.

2. Release the mouse to dock the pane at its current position.

Moving a Pane to a Docked Inner Position

If you drag the pane to one of the inner layout elements, the pane will be positioned along one side of one of the other panes.

1. Drag the pane to one of the inner layout elements.

   Tip: Before you release the mouse, the pane's new position is indicated by a gray area.

2. Release the mouse to dock the pane at its current position.

Moving a Pane to a Shared Position

You can move a pane into another pane's position so two or more panes share the same position:

1. Drag the pane to the center layout element of the pane which position you want to share.

   Tip: Before you release the mouse, the pane's new position is indicated by a gray area.

2. Release the mouse to dock the pane at its current position.

   Tip: To view the content of the panes, click the tabs on the bottom of the shared position.

Splitting Shared Positions

If you do not want a pane to share a position with another pane, do this:

1. Click the tab of the relevant pane and drag it to a new position.

   The pane's new position can be a docked position or a floating pane.

2. Release the mouse to place the pane at its current position.

Using Auto-Hide

You can auto-hide panes. An auto-hidden pane is available as a tab to the right or left of the previous position of the pane. When you place your mouse pointer over the tab, the content of the pane slides out. As soon the cursor is positioned outside the pane, it slides back.

To auto-hide a pane click the *Auto Hide* pushpin in the title bar of the pane you want to auto-hide.

Do the following to show and open an auto-hidden pane again:

1. Place your mouse pointer over the tab of the auto-hidden pane to show the pane.
2. Click the *Auto Hide* pushpin in the title bar of the pane to dock the pane.

Resetting to Default Layout

If you have moved, resized and auto-hidden panes and now want to reset the entire layout of the panes in the Management Client to their default settings, do the following:

1. From the Management Client's *View* menu, select *Reset Application Layout*.
2. Restart the application.

Toggling Preview Pane On and Off

You can close the preview pane when working with recorders and devices by clicking *Close* in the right side of the Preview pane's title bar.

To reopen the Preview pane (see "Panes Overview" on page 36) select *Preview Window* from the Management Client's *View* menu.

Tip: If the preview pane displays images from many cameras at a high frame rate, it may slow down performance. To specify the number of preview images you want in your preview pane, as well as their frame rate, select *Options > General* from the *Tools* menu.

Tip: When the preview pane is closed, it uses no resources and improves therefore the computer's performance.

Activate Licenses

You cannot activate more licenses than you have purchased. To view your total number of licenses, expand *Basics* in the Management Client's Site Navigation pane, and select License Information. If you have added more cameras than you have licenses for, you must get additional licenses before you can activate them.

- Activate Licenses Online (on page 44)
- Activate Licenses Offline (on page 44)
- Activating Licenses after the Grace Day Period (on page 44)

Activate OnSSI License Portal Account

Before you can use the online license function, you must obtain an OnSSI License Portal account. This step need only be done once.

1. To register with the OnSSI Licensing Portal, open a browser and go to the following URL:

   https://rclicensing.onssi.com/CustomerRegistration

2. On the OnSSI Licensing screen, enter your email address. This will become your user name for the OnSSI Licensing Portal.
3. Enter the SLC for RC-E. This is the alphanumeric value found on the license file. For instance, the code should have 11 characters and be in the form similar to: 750-XXXX-XXXX.
4. Click **Submit**.
5. You will receive an email with your OnSSI Licensing Portal user name and password. Use these credentials when activating licenses online.

Activate Licenses Online

1. In the Management Client (RC-E Manager's) Site Navigation pane, expand *Basics*, right-click *License Information*, and select *Activate License Online*.
2. Enter your OnSSI License Portal username and password.
3. Click OK.

Activate Licenses Offline

1. In the Management Client's Site Navigation pane, expand *Basics*, right-click *License Information*, and select *Activate License Offline > Export License for Activation*.

   This will open a *Save Request File* dialog box. A default filename is display. You may keep this filename or change it. The file that will be created is a *license request file* with .lrq filename extension. Save the file to a location that is easily accessible.
2. Click Save to create and save the file.
3. Send the license request file by e-mail to support@onssi.com.

   Your license request will be verified and activated and an updated license file will be sent back to you via e-mail. This process typically takes less than 24 hours. However, during busy peak periods or during weekends or holidays, the process may take 48 hours or more. Please plan ahead.
4. When you have received the updated license file (.lic), save it to a location easily accessible from the Management Client (RC-E Manager).
5. In the RC-E Manager's site navigation pane, expand *Basics*.
6. Right-click *License Information*, select *Activate License Offline > Import Activated License* and select the .lic file to import it.
7. Click Open to import the file and complete the activation process.

Activating Licenses after the Grace Day Period

If the grace day period is reached before activation, all cameras which are not activated within the given period will become unavailable, and will not be able to send data to the surveillance system.

If you exceed the grace day period before you activate a license, the license is not lost. You can activate the license as usual using either of the above steps (Activating Licenses Online or Offline).

Configuration, added cameras, defined recording servers, and other settings will not be removed from the Management Client if a license is activated too late.

Manage Licenses

When you purchase RC-E, you also purchase a certain number of licenses for device channels. Device channels are typically cameras but could also be dedicated input/output boxes.

At first, when you have installed the various RC-E components, configured the system, and added recording servers and cameras through the Management Client, the surveillance system runs on temporary licenses which need to be activated before a certain period ends. This is called the 'grace day period'.

When the new surveillance system is working, we recommend that you activate your licenses before you make the final adjustments. The reason is that you must activate your licenses before the grace day period expires, since all recording servers and cameras for which no licenses have been activated will not be able to send data to the surveillance system if the grace day period is expired.

Which Devices Require a License?

You need licenses for the number of device channels - typically cameras but it could also be dedicated input/out boxes - you want to run on the RC-E system. One device channel license enables you to run one camera or one dedicated input/output box. You can use and define an unlimited number of recording servers, microphones, speakers, inputs and outputs.

You can always get more licenses as your surveillance system grows. See Getting Additional Licenses (on page 46).

What to Know When Replacing Cameras?

You can replace a camera licensed in the RC-E system with a new camera, and have the new camera activated and licensed instead.

The total number of purchased device channels corresponds to the total number of cameras that are able to run on the surveillance system simultaneously. If you remove a camera from a recording server, you also free a license.

If you replace a camera with a similar camera (manufacturer, brand, and model), and give the new camera the same IP address as the old one, you will maintain full access to all the camera's databases. In this case, you simply move the network cable from the old camera to the new one without changing any settings in the Management Client, and then activate the license.

If replacing a camera with a different model, you must use the Management Client's *Replace Hardware* wizard to map all relevant databases of cameras, microphones, inputs, outputs, etc. When done, remember to activate the license. For details on the *Replace Hardware* wizard*, s*ee Replacing Hardware (on page 54).

There is no limit to the number of cameras you can replace.

What to Know about Licenses and OnSSI Federated Architecture?

Refer to OnSSI Federated Architecture Overview (on page 173)

Viewing Your License Information

A comprehensive overview of the licenses in your RC-E recorder is available if you expand *Basics* in the RC-E Manager's Site Navigation pane (see "Panes Overview" on page 36), and then select *License Information*. This will bring up the *License Information* page, on which you can see:

- Your software license code
- The total number of available device channels (typically cameras but it could also be dedicated input/output boxes) you are licensed to run

- How many licenses you have used, both the number of activated licenses and the number of temporary (not activated) licenses
- Whether you need to get additional licenses in order to have enough licenses for all of your cameras

Any expiry dates listed on the page are in the management server's local time. Since you are not necessarily located in the same time zone as the management server, the management server's current local time is displayed in the bottom right corner of the page.

You can activate licenses online or offline, by expanding *Basics* in the Site Navigation pane, and right-clicking *License Information*.

The cameras (or dedicated input/output boxes) for which you do not have a license will not send data to the surveillance system. Cameras added after all available licenses are used are unavailable. Cameras without licenses will be identified by an exclamation mark symbol when listed in the Management Client's overview pane (see "Panes Overview" on page 36).

Tip: In the short period until you have obtained additional licenses, you can disable some less important cameras to allow some of the new cameras to run instead. See Manage Hardware (on page 53) for more information.

Where I Can See How Many Grace Days I Have Left? This information is also available from the *License Information* page where you can see if you need to get more licenses so all added cameras can deliver data to RC-E. When you add a new camera for which you have a license, you are granted a new full grace day period for the camera in question from the date you added the camera. Therefore the end date of the grace day period displayed on the *License information* page is for the first added but not activated camera. The duration of the full grace day period can be found in a *readme* file which is available from Windows' Start menu, by selecting *All Programs > RC-E > Read Me*.

Getting Additional Licenses

What if you want to add - or if you already have added - more device channels (cameras or dedicated input/output boxes) than you currently have licenses for? In that case, you must buy additional licenses before the cameras will be able to send data to your RC-E system.

To get additional licenses for RC-E, contact your OnSSI vendor, or visit www.onssi.com (http://www.onssi.com).

When you have received an updated license file (.lic) with the new licenses, you can activate your licenses.

Tip: In the short period until you get the additional licenses, you can disable some less important cameras to allow some of the new cameras to run instead. To disable or enable a camera, expand *Recording Servers* in Management Client's Site Navigation pane (see "Panes Overview" on page 36), then select the required recording server, right-click the required camera, and select *Enable*.

Remote Connect Services

About Remote Connect Services

The Remote Connect Services feature contains the Axis One-click Camera Connection technology developed by Axis Communications. It enables RC-E to retrieve video (and audio) from external cameras where firewalls and/or router network configuration normally prevents initiating connections to such cameras. The actual communication takes place via 'secure tunnel servers' (ST servers).

ST servers use a Virtual Private Network (VPN). Only devices holding a valid key can operate within a VPN. This offers a secure tunnel where data can be exchanged between public networks in a safe way.

Remote Connect Services allows you to...

- Edit credentials within the Axis Dispatch Service

- Add, edit, and remove ST servers
- Register/Unregister and edit Axis One-click cameras
- Go to the hardware related to the Axis One-Click camera.

Before you can use Axis One-click Camera Connection, you must first **install a suitable ST server environment**.

Installing an STS Environment for One-click Camera Connection

1. Contact your system provider to obtain the needed user name and password for Axis Dispatch Services
2. Make sure your camera(s) support Axis Video Hosting System, http://www.axis.com/products/avhs/ (http://www.axis.com/products/avhs/).
3. If needed, update your Axis cameras with the newest firmware, http://www.axis.com/techsup/firmware.php (http://www.axis.com/techsup/firmware.php)
4. On each camera's homepage, go to *Basic Setup*, *TCP/IP*, and select *Enable AVHS* and *Always*
5. From your management server's built-in download web page, install the *Axis One-Click Connection Component* to setup a suitable Axis secure tunnel framework
6. Start the *Axis One-Click service* from Services(search for *services.msc* on your machine).

Working with Axis One-click Camera

Editing the Axis Dispatch Service Properties

1. The Properties pane displays relevant dispatch information on the *Axis Dispatch Service* tab.
2. Edit properties (see "Axis One-Click Camera Connection Properties" on page 48).
3. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

Adding or Editing Secure Tunnel Servers

1. Do one of the following:

a) To add an ST server, right-click the *Axis Secure Tunnel Servers* node, select *Add Axis Secure Tunnel Server...*

or

b) To edit an ST server, right-click it, select *Edit Axis Secure Tunnel Server...*

2. In the window that opens, fill in the relevant information (see "Axis One-Click Camera Connection Properties" on page 48).
3. If you chose to use credentials when you installed the *Axis One-Click Connection Component*, make sure to select the *Use credentials* check box and fill in exactly the same user name and password as used for the *Axis One-Click Connection Component*.
4. Click *OK*.

Removing Secure Tunnel Servers

1. To remove an ST server, right-click it, select *Remove Axis Secure Tunnel Server...*
2. Click *Yes*.

Registering a new Axis One-click Camera

1. To register a camera under an ST server, right-click it, select *Register Axis One-click Camera...*
2. In the window that opens, fill in the relevant information (see "Axis One-Click Camera Connection Properties" on page 48).
3. Click *OK*.
4. The camera will now appear under the relevant ST server.

The color coding of the camera is either:

- **Red:** Initial state—registered, but not connected to the ST server
- **Yellow:** Registered—connected to the ST server, but not added as hardware
- **Green:** Added as hardware—may or may not be connected to the ST server.

When added, status will always be green. The connection status (see "Read Server Service State Icons" on page 199) is then—as normal—reflected by *Devices* on *Recording Servers* in the overview pane.

In the overview pane, you may group your cameras for an easier overview.

If you choose **not** to register your camera at the Axis dispatch service at this point, you can do so later from the right-click menu (select *Edit Axis One-click Camera...*).

Unregistering an Axis One-click Camera

1. To unregister a camera under an ST server, right-click it, select *Unregister Axis One-click Camera.*
2. In the dialog that appears, make sure the check mark is selected and click *Yes*.
3. The camera will disappear from under the relevant ST server.

Axis One-Click Camera Connection Properties

- ***Camera password:*** Enter/Edit. Provided with your camera at purchase. For further details, see your camera's manual or www.axis.com (http://www.axis.com).
- ***Camera user:*** See details for *Camera password.*
- ***Description:*** Enter/Edit a description of the item. Not required.
- ***External address:*** Enter/Edit the http address of the ST server where the camera(s) connect.
- ***Internal address:*** Enter/Edit the http address of the ST server where the recording server connects.

  Tip: Remember *http://* in front of both the external and internal address.
- ***Name:*** If needed, edit the name of the item.

- ***Owner authentication key:*** See *Camera password.*
- ***Passwords*** (for Dispatch Server)***:*** Enter password. Must be identical to the one received from OnSSI.
- ***Passwords*** (for ST server)***:*** Enter password. Must be identical to the one entered when the *Axis One-Click Connection Component* was installed.
- ***Register/Unregister at the Axis Dispatch Service:*** Indicate whether you wish to register your Axis camera with the Axis dispatch service. Can be done at time of setup or later.
- ***Serial number:*** Same as the MAC address. See *Camera password.*
- ***Use credentials:*** If it was decided—during installation of the ST server—to use credentials, select the check box.
- ***User name*** (for Dispatch Server)***:*** Enter user name. Must be identical to the one received from OnSSI.
- ***User name*** (for ST server)***:*** Enter user name. Must be identical to the one entered when the *Axis One-Click Connection Component* was installed.

Servers

Add Hardware (Cameras, etc.)

The *Add Hardware* wizard helps you detect IP hardware devices, such as cameras and video encoders, on your network and add them to recording servers on your RC-E system.

To access *Add Hardware*, expand the *Servers* folder in the Management Client's Site Navigation pane (see "Panes Overview" on page 36) and select the *Recording Server* node, then in the overview pane (see "Panes Overview" on page 36) right-click the required recording server and select *Add Hardware...*

The wizard offers you four ways of detecting and adding hardware devices: *Express (recommended)*, *Address range scanning, Manual* and *Remote connect hardware*. With the *Express* option, RC-E automatically scans for available hardware on the recording server's local network. With *Address range scanning, RC-E scans defined network IP address ranges and detects hardware models. With Manual*, you manually specify the IP address and port for each device. With *Remote connect hardware*, you can add hardware connected via a remotely connected server. All options offer the possibility of automatically detecting the correct hardware drivers.

Tip: If you are new to RC-E: use the *Express* hardware detection as it will guide you through each of the steps involved in detecting and adding your IP devices.

It is strongly advised that you **only** add a physical hardware device to **one recording server** at the time.

Express

The *Express (recommended)* option automatically discovers hardware models on the recording server's local network.

1. Select *Express (recommended)* and click *Next*.
2. Specify user names and passwords if your hardware devices are not using the factory default user name and password. You can add as many user names and passwords as required by clicking *Add*. Remember to select the *Include* check box for each required device.

   When ready, click *Next*.
3. Wait while the hardware is detected. A status indicator will show the detection process.

Tip: Select the *Show hardware running on other recording servers* check box to see if detected hardware is running on other recording servers.

Once detection is complete, click *Next*.

4. Wait while device-specific information is collected for each hardware device. A status indicator will show the detection process. If collecting hardware information for a device is unsuccessful, click the *Failed* error message to see why. Once collection is complete, click *Next*.

   Choose to enable or disable successfully detected hardware and cameras. Detected hardware, such as hardware device, camera, microphone and speaker is listed individually, allowing you to, for example, add a hardware device's camera without enabling its speaker if needed.

   You can change the name of the hardware by clicking *Hardware name* and choosing between:

   - *[Hardware model] [address]*
   - *[Hardware model]*

   Additionally, you can change name of the device by clicking *Device name* and choosing between:

   - *[Hardware name] - [Device type] [number]*
   - *[Device type] [number] on [hardware name]*
   - *[Address] - [Device type] [number]*

   A change of name for hardware and/or device will be applied to all available hardware/devices and will take effect immediately.

   Tip: You can disable the hardware, but enable its devices if necessary.

   When ready, click *Next*.

5. Select a default group for all device types, or group the devices individually. The devices are listed according to type, for example, camera, microphone, speaker. Click *Finish*.

Address Range Scanning

The *Address Range Scanning* option scans your network for relevant hardware devices based on your specifications regarding required IP ranges, drivers, and device user names and passwords.

1. Select *Address Range Scanning* and click *Next*.
2. Specify user names and passwords if your hardware devices are not using the factory default user name and password. You can add as many user names and passwords as required by clicking *Add* . Remember to select the *Include* check box for each required device. You must add and include at least one user name and password in order for the wizard to proceed.

   When ready, click *Next*.

3. Select which drivers to use when scanning. By default, RC-E will use all known drivers. If your organization only uses certain hardware devices and/or models, you can achieve faster scanning by selecting only the drivers required for those hardware devices. Click *Next*.

   Tip: The list of drivers is typically very long, and by default all drivers are selected. With *Select All* and *Clear All*, you can avoid having to select/clear all check boxes manually.

4. Specify the IP address network ranges you want to scan for hardware.

- **Start address**: First IP address in required range.
- **End address:** Last IP address in required range. The start and end IP address may be identical, allowing you to only scan for a single hardware device if needed.
- **Port:** Port number(s) on which to scan. Default is port 80. If your hardware devices are located behind a NAT-enabled router or a firewall, you may need to specify a different port number. When this is the case, also remember to configure the router/firewall so it maps the port and IP addresses used by the hardware devices.

You can add as many network ranges as needed by clicking *Add* to add another row. You can add any network address between 0.0.0.1 and 255.255.255.255. At least one network range must be selected before you can continue.

Remember to select the *Include* check box for each required range.

You can only specify IPv4 addresses when using *Address Range Scanning*.

Wait while the hardware is detected. A status indicator will show the detection process.

If you successfully detect hardware on a specified network range, a *Success* message will appear in the *Status* column. If you fail to add a network range, you can click the *Failed* error message to see why.

Tip: Select the *Show hardware running on other recording servers* check box to see if detected hardware is running on other recording servers.

Once detection is complete, click *Next*.

5. Wait while device-specific information is collected for each hardware device. A status indicator will show the detection process. If collecting hardware information for a device is unsuccessful, click the *Failed* error message to see why the collection of information has failed. Once collection is complete, click *Next*.
6. Choose to enable or disable successfully detected hardware and cameras. Detected hardware, such as hardware device, camera, microphone and speaker is listed individually, allowing you to, for example, add a hardware device's camera without enabling its speaker if needed.

   You can change the name of the hardware by clicking *Hardware name* and choosing between:

   - *[Hardware model] [address]*
   - *[Hardware model]*

   Additionally, you can change name of the device by clicking *Device name* and choosing between:

   - *[Hardware name] - [Device type] [number]*
   - *[Device type] [number] on [hardware name]*
   - *[Address] - [Device type] [number]*

   A change of name for hardware and/or device will be applied to all available hardware/devices and will take effect immediately.

   Tip: You can disable the hardware, but enable its devices if necessary.

   When ready, click *Next*.
7. Select a default group for all device types. The devices are listed according to type, for example, camera, microphone, speaker. Click *Finish.*

Manual

The *Manual* option lets you specify details about each hardware device separately. This can be a good choice if you only want to add a few hardware devices, and you know their IP addresses, required user names and passwords, etc.

1. Select *Manual* and click *Next*.
2. Specify user names and passwords if your hardware devices are not using the factory default user name and password. You can add as many user names and passwords as required by clicking *Add*. Remember to select the *Include* check box for each required device. You must choose to add and include at least one user name and password in order for the wizard to proceed.

   When ready, click *Next*.
3. Now select which drivers to use when scanning. By default, RC-E will use all known drivers. If your organization only uses certain hardware devices and/or models, you can achieve faster scanning by selecting only the drivers required for those hardware devices.

   Tip: The list of drivers is typically very long, and by default all drivers are selected. With *Select All* and *Clear All* , you can avoid having to select/clear all check boxes manually.

   When ready, click *Next*.
4. Specify information for the hardware you want to add. You can also optionally select the type of driver you want to add to speed up hardware detection.
   - ***Address:*** Specify the IP address of the hardware, you want to add.
   - ***Port:*** Specify the port number to which the camera is added.
   - ***Hardware driver:*** Select the driver of the hardware you want to add. Or select *Auto-detect* to let the wizard detect which driver to install.
5. Wait while the hardware is detected. A status indicator will show the detection process. Select or clear the network ranges to use in the detection process.

   If you successfully detect hardware, a *Success* message will appear in the *Status* column. If you fail to add a network range, click the *Failed* error message to see why.

   Tip: Select the *Show hardware running on other recording servers* check box to see if detected hardware is running on other recording servers.

   Once detection is complete, click *Next*.
6. Choose to enable or disable successfully detected hardware and cameras. Detected hardware, such as hardware device, camera, microphone and speaker is listed individually, allowing you to, for example, add a hardware device's camera without enabling its speaker if needed.

   You can change the name of the hardware by clicking *Hardware name* and choosing between:
   - *[Hardware model] [address]*
   - *[Hardware model]*

   Additionally, you can change name of the device by clicking *Device name* and choosing between:
   - *[Hardware name] - [Device type] [number]*
   - *[Device type] [number] on [hardware name]*
   - *[Address] - [Device type] [number]*

A change of name for hardware and/or device will be applied to all available hardware/devices and will take effect immediately.

Tip: You can disable the hardware, but enable its devices if necessary.

When ready, click *Next*.

7. Select a default group for all device types or group the devices individually. The devices are listed according to type, for example, camera, microphone, speaker. Click *Finish.*

Remote Connect Hardware

Remote connect hardware automatically scans for hardware connected via a remotely connected server.

1. Select *Remote connect hardware* and click *Next*.
2. Wait while the hardware is detected. A status indicator will show you how far you are in the detection process.
3. Once detection has completed, select which hardware you want to add and click *Next*.

Manage Hardware

For each recording server on your system, you have several options for managing added IP hardware.

Most configuration and management of individual camera settings (such as a camera's recording settings), input settings, and output settings takes place on a more detailed level; see Manage Cameras (on page 75), Manage Inputs (see "Manage Input" on page 88), and Manage Outputs (see "Manage Output" on page 91).

Editing Basic Hardware Settings (IP, etc.)

You are able to edit basic settings, such as IP address/host name, for added hardware:

1. In the overview pane (see "Panes Overview" on page 36), expand the required recording server, right-click the hardware device you wish to edit.
2. From the menu that appears, select *Edit IP Hardware...*:

   This opens the *Edit Hardware* window, in which you can edit the following:

   - ***Name***: The name of the hardware in the Management Client's lists, etc.

   Tip: You can also quickly change the name of a hardware device by selecting *Rename IP Hardware...* from the menu.

   - ***Description***: (Optional) A description or other information about the hardware device. It will, among other places, appear when you pause your mouse pointer over the hardware device in the overview pane.
   - ***Hardware URL:*** URL, IP address, or host name of the hardware device.
   - ***User name:*** Required to access and use the hardware device.
   - ***Password***: Required to access and use the hardware device.
   - ***Type***: Non-editable field indicating the hardware driver used for the hardware device.
3. Click *OK*.

Deleting Individual Hardware

IMPORTANT: When deleting a hardware device, all its recordings are deleted permanently.

1. In the overview pane (see "Panes Overview" on page 36), expand the required recording server, right-click the no longer needed hardware device.
2. From the menu that appears, select *Delete IP Hardware.*

   Tip: As an alternative, press DELETE on your keyboard.
3. Confirm that you want to delete the hardware device.
4. The hardware device is removed from the recording server's listings in the Management Client.

Tip: If you ever need to add the hardware device to a recording server again, select the required recording server and use the Add Hardware (see "Add Hardware (Cameras, etc.)" on page 49) wizard.

Replacing Hardware

When you replace a physical camera (hardware device) on your network with another hardware device, you must know the IP address, port, user name and password of the new hardware device.

Furthermore, when replacing hardware devices, note that your system might be affected by license limitations (see "Manage Licenses" on page 45). Using the *Activate Online* (see "*Activate Licenses*" on page 43)wizard, you must reactivate your licenses **after** replacing hardware devices. Also note, that if the new number of cameras, microphones, inputs, outputs, etc. exceeds the old number of cameras, microphones, inputs, outputs, etc. you might also have to buy new licenses (see "Manage Licenses" on page 45). See your License Information (see "Manage Licenses" on page 45).

1. In the Overview pane (see "Panes Overview" on page 36), expand the required recording server, right-click the hardware device you wish to replace.
2. From the menu that appears, select *Replace Hardware.*
3. The *Replace Hardware* wizard appears. Click *Next*.
4. In the wizard, in the *Address* field (marked by red arrow in the image), enter the IP address of the new hardware. If known, select relevant hardware device driver from the *Hardware Driver* drop-down list (marked by red arrow in the image). Otherwise select *Auto Detect*. If port, user name or/and password data is different for the new device, also correct this **before starting the auto detect process (if needed)**.

   Tip: The wizard is pre-filled with data from the existing hardware device. If you replace it with a similar hardware device, you can reuse some of this data - for example, port and driver information.
5. Do one of the following:

   - If you selected the required hardware device driver directly from the list, click *Next*.
   - If you selected *Auto Detect* in the list, click *Auto Detect*, wait for this process to be successful, click *Next*.

   This step is designed to help you map devices and their databases, depending on the number of individual cameras, microphones, inputs, outputs, etc., attached to the old hardware device and the new respectively.

   It is important to consider **how** to map databases from the old hardware device to databases of the new hardware device. You do the actual mapping of individual cameras, microphones, inputs, outputs, etc. by selecting a corresponding camera, microphone, input, output or *None* in the right-side column.

   IMPORTANT: Make sure to map **all** cameras, microphones, inputs, outputs, etc. Contents stored in databases belonging to cameras, microphones, inputs, outputs, etc. mapped to *None*, will be **lost**.

Click *Next*.

6. You are presented with a list of hardware to be added, replaced or removed. Click *Confirm*.
7. Final step is a summary of added, replaced and inherited devices and their settings. Click *Copy to Clipboard* to copy contents to an external source (for, for example, reporting purposes) or/and *Close* to end the wizard.

Renaming Hardware

1. In the overview pane (see "Panes Overview" on page 36), expand the required recording server, right-click the hardware device you wish to rename.
2. From the menu that appears, select *Rename IP Hardware.*

   Tip: As an alternative, press F2 on your keyboard.
3. Overwrite the name of the hardware.

Disabling/Enabling Hardware

Added hardware is by default **enabled**.

In the overview pane (see "Panes Overview" on page 36), under the required recording server, enabled/disabled hardware devices are indicated.

Disabling

Disable added hardware, for example, for licensing or performance purposes:

1. In the overview pane (see "Panes Overview" on page 36), expand the required recording server, right-click the hardware device you wish to disable.
2. From the menu that appears, select *Enabled* to clear it.

Deleting All Hardware on a Recording Server

IMPORTANT: When deleting hardware devices, all recordings from the hardware devices in question will be deleted permanently.

1. In the overview pane (see "Panes Overview" on page 36), right-click the required recording server where you want to delete all hardware.
2. From the menu that appears, select *Delete All Hardware.*
3. Confirm that you want to delete all hardware on the selected recording server.

Renaming Individual Devices

1. In the overview pane (see "Panes Overview" on page 36), expand the required recording server and the required hardware device. Right-click the camera, input, or output you wish to rename.
2. From the menu that appears, select *Rename Device.*

   Tip: As an alternative, press F2 on your keyboard.
3. Overwrite the name of the selected device.

Enabling/Disabling Individual Devices

Cameras are by default **enabled**. **Microphones, speakers, inputs** and **outputs** are by default **disabled**.

This means that microphones, speakers, inputs and outputs must be individually enabled before they can be used on the RC-E system. The reason for this is that surveillance systems inherently rely on cameras, whereas the use of microphones, etc. is highly individual depending on organizations' needs.

In the overview pane (see "Panes Overview" on page 36), under the required server, enabled/disabled devices are indicated:

The same method for enabling/disabling is used for cameras, microphones, speakers, inputs, and outputs.

Enabling

1. In the overview pane (see "Panes Overview" on page 36), expand the required recording server and the required hardware device. Right-click the camera, input, or output you wish to enable.
2. From the menu that appears, select *Enabled.*

About Storage and Archiving

When a camera or device records video and/or audio, all specified recordings are per default stored in the storage area defined for the device. More precisely in the storage area's default recording database named *Recording*. A storage area has no default archive(s), but these can easily be created.

Depending on recording settings, the storage areas's recording database will most likely run full at some point and its contents need to be archived in order to be saved. It is therefore possible to create archives within the default storage area and start an archiving process. Furthermore, it is possible to create alternative storage area(s) and configure that selected video/audio recordings must be stored/archived here.

Archiving is the automatic transfer of recordings from a camera's or device's default database to another location. This way, the amount of recordings you are able to store will not be limited by the size of the device's recording database. Archiving also makes it possible to back up your recordings on backup media of your choice.

Storage and archiving is configured on a per-recording server basis.

To ease explanations, the following mostly mentions cameras and video, but al is true about speakers and microphones and audio and sound as well.

IMPORTANT: We recommend that you use a dedicated hard disk drive for the recording server database. Using a dedicated hard disk drive for the database will prevent low disk performance. Furthermore, when formatting the hard disk, it is important to change its *Allocation unit size* setting from 4 to 64 kilobytes. This is to significantly improve recording performance of the hard disk. You can read more about allocating unit sizes and find help at http://support.microsoft.com/kb/140365/en-us (see http://support.microsoft.com/kb/140365/en-us - http://support.microsoft.com/kb/140365/en-us).

IMPORTANT: The oldest data in a database will always be auto-archived (or deleted if no next archive is defined) when less than 5GB of space is free. If less than 1GB space is free, data will be deleted. A database always requires 250MB of free space; if this limit is reached (if data is not deleted fast enough), no more data will be written to the database until enough space has been freed. The actual maximum size of your database will thus be the amount of gigabytes you specify, minus 5GB.

Attaching Devices to a Recording Server

Once you have configured the storage area and archiving settings for a recording server (where to store recordings, archives, how often to transfer recordings to archives, etc.), you can enable storage and archiving for individual

cameras or a group of cameras. This is done from the individual devices or from the device group, see Attaching Individual Devices or a Group of Devices to a Storage Area (on page 58).

Effective Archiving

When archiving is enabled for a camera or a group of cameras, the contents of the camera(s)' database will automatically be moved to an archive at regular intervals.

Depending on your requirements, you are able to configure one or more archives for each of your databases. Archives can be located either on the recording server computer itself, or at another location which can be reached by RC-E , for example on a network drive.

By setting up your archiving in an effective way, you can prune and groom your database storage area usage significantly if needed. Often, it is desired to make archived recordings take up as little space as possible—especially on a long-term basis, where it is perhaps even possible to slacken image and sound quality a bit. Effective pruning and grooming can help ensure this and can be handled from the *Storage* tab (see "Storage Tab (Recording Server Properties)" on page 65) of a recording server by adjusting several interdependent settings such as:

- Recording database retention
- Recording database size
- Archive retention
- Archive size
- Archive schedule
- Encryption
- Frames Per Second (FPS).

The size fields define the size of the camera's database, exemplified by the cylinder, and its archive(s) respectively:

By means of retention time and size setting for the recording database, exemplified by the white area in the cylinder, you define how old recordings must be before they are archived. In our illustrated example, recordings are archived when they have "sifted" down into the green area of the database cylinder, or in other words: when they are old enough to be archived.

The retention time and size setting for archives define how long the recordings remain in the archive; recordings remain in the archive for the time specified, or until the archive has reached the specified size limit. When these settings are met, RC-E begins to overwrite old recordings in the archive.

The archiving schedule defines how often and at what times archiving takes place.

Encryption and FPS determine the size of the data in the databases.

To have recordings archived, all these parameters must be set up in accordance with each other. This means that the retention period of a next coming archive must always be longer than the retention period of a current archive or recording database. This is due to the fact that the number of retention days stated for an archive includes all retention stated earlier in the process. Furthermore, archiving must always take place more frequently than the retention period is set to, otherwise you risk losing data. If you have a retention time of 24 hours, any data older than 24 hours will be deleted. Therefore, to get your data safely moved to the next archive, it is important to run archiving more often than every 24 hours.

> ***Example:*** These storage areas (image to the left) has a retention time of 4 days and the following archive (image to the right) a retention time of 10 days. Furthermore, archiving is set to occur every day at 10:30, ensuring a much more frequent archiving than retention time is set to.

Tip: You can also control archiving by use of rules and events. See About Rules and Events (see "About Events" on page 97) and Events Overview (on page 128).

Attaching Individual Devices or a Group of Devices to a Storage Area

Once a storage area is configured for a recording server, you can enable it for individual devices (cameras, microphones or speakers) or a group of devices. You can also select which of a recording server's storage areas should be used for the individual device or the group.

1. In the Site Navigation pane (see "Panes Overview" on page 36), expand *Devices* and select either *Cameras*, *Microphones* or *Speakers* as required.
2. In the Overview pane (see "Panes Overview" on page 36), select the required device or a device group.
3. In the Properties pane, select the *Record* tab.
4. In the *Storage* area, select *Select...*
5. In the dialog that appears, select the wanted database, click *OK*.
6. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

Viewing Archived Recordings

Archived recordings may be viewed in the Ocularis Client. As long as the archived recordings are stored locally or on accessible network drives, you can use the Ocularis Client's many features (kinetic timeline, motion slicing, evidence export, etc.) when browsing archived recordings; just like you would with recordings stored in a cameras' regular databases. The fact that you are viewing archived recordings will be completely transparent.

Remember that individual user rights may prevent particular users from viewing recordings from particular cameras - just as is the case when browsing recordings from cameras' regular databases.

Backing Up Archived Recordings

Many organizations want to back up their recordings, using tape drives or similar. Exactly how you do this is highly individual, depending on the backup media used in your organization. However, the following is worth bearing in mind:

Back Up Archives Rather than Camera Databases

Always create backups based on the content of archives, not based on individual camera databases. Creating backups based on the content of individual camera databases may cause sharing violations or other malfunctions.

When scheduling a backup, make sure the backup job does not overlap with your specified archiving times.

Tip: You are able to view each recording server's archiving schedule in each of a recording server's archives, on the Storage tab (see "Storage Tab (Recording Server Properties)" on page 65).

Knowing Archive Structure Lets You Target Backups

When recordings are archived, they are stored in a certain sub-directory structure within the archive.

During all regular use of your RC-E system, the sub-directory structure will be completely transparent to the system's users, as they browse all recordings with the Ocularis Client regardless of whether the recordings are archived or not. Knowing the sub-directory structure is thus primarily interesting if you want to back up your archived recordings (see "Archive Structure" on page 59).

Using the Ocularis Client to View Archived Video

You can use the Ocularis Client to view archived video. See the Ocularis Client documentation for details.

Archive Structure

When recordings are archived, they are stored in a certain sub-directory structure within the archive.

During all regular use of your RC-E system, the sub-directory structure will be completely transparent to the system's users, as they browse all recordings with the Ocularis Client regardless of whether the recordings are archived or not. Knowing the sub-directory structure is thus primarily interesting if you want to back up your archived recordings.

In each of the recording server's archive directories, separate sub-directories are automatically created. These sub-directories are named after the name of the device and the name of the archive database.

Since you are able to store recordings from different cameras in the same archive, and since archiving for each camera is likely to be performed at regular intervals, further sub-directories are also automatically added.

These sub-directories each represent approximately an hour's worth of recordings. The one-hour split makes it possible to remove only relatively small parts of an archive's data if the maximum allowed size of the archive is reached.

The sub-directories are named after the device, followed by an indication of whether recordings come from an edge camera or via SMTP (if relevant), *plus* the date and time of the most recent database record contained in the sub-directory.

Naming structure:

```
...[Storage Path]\[Storage name]\[device-name] - plus date and time of most
recent recording]\
```

If from edge camera:

```
...[Storage Path]\[Storage name]\[device-name] (Edge) - plus date and time of
most recent recording]\
```

If from SMTP:

```
...[Storage Path]\[Storage name]\[device-name] (SMTP) - plus date and time of
most recent recording]\
```

Real life example:

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Server(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

Even further sub-directories are automatically added. The amount and nature of these sub-directories depend on the nature of the actual recordings. For example, several different such sub-directories will be added if the recordings are technically divided into sequences; something which is often the case if motion detection has been used to trigger recordings.

If you want to back up your archives, knowing the basics of the sub-directory structure enables you to target your backups.

Examples:

If wishing to back up the content of an entire archive, back up the required archive directory and all of its content; for example everything under:

```
...F:\OurArchive\
```

If wishing to only back up the recordings from a particular camera from a particular period of time, back up the contents of the relevant sub-directories only; for example everything under:

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Server(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

Archiving and Virus Scanning

If you are using virus scanning software on the computer on which the camera databases you want to archive are located, or on a computer to which data is archived, it is likely that the virus scanning will use a considerable amount of system resources on scanning all the data which is being archived.

This may affect system performance negatively. Also, virus scanning software may temporarily lock each file it scans, which may further impact system performance negatively.

If possible, you should therefore disable any virus scanning of camera databases and archiving locations.

Frequently Asked Questions about Archiving

What happens if a storage area becomes unavailable? If a storage area becomes unavailable-for example if the storage area is located on a network drive, and the connection to the drive is lost— it will not be possible to store recordings in the storage area. RC-E registers the availability of its recording servers' storage areas. This means that when a storage area becomes available again, it will again be possible to save recordings in the storage area. However, any recordings from the period in which the storage area was unavailable will be lost. When creating rules (see "Manage Rules" on page 133), you can use the events *Database Storage Area Unavailable* and *Database Storage Area Available* to trigger actions, such as the automatic sending of e-mail to relevant people in your organization (see Events Overview (on page 128) for more information). Furthermore, information about a storage area becoming unavailable/available will be logged (see "Manage Logs" on page 158).

How do I ensure that archiving is set up correctly? Archives are set up by adjusting several interdependent parameters correctly as described previously.

Can I create an archive on a network drive? Archives can be located either on the recording server computer itself, or at another location which can be reached by RC-E, for example on a network drive.

What happens when the maximum size of an archive is reached? When you create archives from the *Storage* tab (see "Storage Tab (Recording Server Properties)" on page 65), you specify a maximum size limit for the archive, in days and gigabytes. When either of the two maximum limits is reached, recordings in excess of the specified number of days/gigabytes will be removed. However, in order not to remove more recordings than necessary, excess recordings will be removed in chunks of approximately one hour's worth of recordings.

What happens if a scheduled archiving fails? If a scheduled archiving fails, for example because the archive is located on a network drive which is temporarily unavailable, RC-E will retry archiving after an hour. If that fails, another retry will take place after yet another hour, and so forth.

If the time of the next scheduled archiving is reached between two retries, an archiving attempt will be made at the scheduled time; if that attempt fails, OnSSI RC-E will retry archiving after an hour, and so forth.

What happens if archiving is not finished before the next scheduled archiving? Your RC-E system inserts a compulsory period of archiving-free time after each finished archiving job. This ensures that archiving jobs do not overlap in time.

Manage Recording Servers

OnSSI RC-E recording servers are used for recording video feeds, and for communicating with cameras and other devices. An RC-E surveillance system will typically contain several recording servers, although only a single recording server is required for the system to work.

Recording servers on your system— i.e. computers with the RC-E recording server software installed, and configured to communicate with an RC-E management server— will be listed in the Management Client's overview pane (see "Panes Overview" on page 36) when you expand the *Servers* folder in the Site Navigation pane (see "Panes Overview" on page 36) and then select the *Recording Servers* node.

Backward compatibility with recording servers from RC-E versions older than 3.0 is limited. You can still access recordings on such older recording servers; but in order for you to be able to change their configuration, they must be

of version 3.0 or later. It is thus highly recommended that all recording servers in your RC-E system are upgraded (see "Upgrade from Previous Version" on page 28) to the latest possible version.

IMPORTANT: When the **Recording Server Service** is running, it is **very** important that neither Windows Explorer nor other programs are accessing Media Database files or folders associated with your OnSSI RC-E surveillance setup. Otherwise, the recording server might not be able to rename or move relevant media files. Unfortunately, this might bring the recording server to a halt. If this situation has already occurred, stop the Recording Server Service, close the program accessing the media file(s) or folder(s) in question, and simply restart the Recording Server Service.

Authorizing a Recording Server

When first using the system, or when new recording servers have been added to the system, you must authorize the new recording servers.

Why must I authorize recording servers? In an RC-E system, recording servers point to management servers, not the other way round. In theory, recording servers which you do not want to include in your surveillance system could thus be configured to connect to your management servers. By authorizing recording servers before they can be used, surveillance system administrators have full control over which recording servers are able to send information to which management servers.

1. Expand the *Servers* folder in the Management Client's Site Navigation pane and select the *Recording Servers* node.
2. Right-click the required recording server in the overview pane.
3. From the menu that appears, select *Authorize Recording Server*:

   After a short moment, the recording server will be authorized and ready for further configuration.

Viewing/Editing a Recording Server's Properties

When a recording server is authorized, you are able to view/edit the recording server's properties, including its database storage area settings:

When you select the required recording server in the Management Client's overview pane, the recording server's properties are displayed in the properties pane (see "Panes Overview" on page 36). Expand the required recording server to see which devices are connected to the recording server. While the Management Client loads information about the recording server, the text *(... expanding)* is displayed next to that recording server:

Adding Hardware (Cameras, etc.) to a Recording Server

You add IP hardware, such as cameras, video encoders, etc., to recording servers on your RC-E system through the *Add Hardware* wizard. The wizard helps you scan your network for relevant hardware. See the wizard *Add Hardware* (see "*Add Hardware (Cameras, etc.)*" on page 49) for more information.

Managing Hardware on a Recording Server

You have several options for managing IP hardware, such as cameras, video encoders, etc., on recording servers on your RC-E system. See Manage IP Hardware (see "Manage Hardware" on page 53).

Renaming a Recording Server

1. Expand the *Servers* folder in the Management Client's Site Navigation pane and select the *Recording Servers* node.

2. Right-click the required recording server listed in the overview pane.
3. From the menu that appears, select *Rename Recording Server*.

   Tip: As an alternative to using the menu, press the F2 key on your keyboard.

4. You are now able to overwrite the name of the recording server in the overview pane.

Removing a Recording Server

IMPORTANT: Removing a recording server will remove all configuration specified for the recording server through the **Management Client, including all** of the recording server's associated hardware (cameras, input devices, etc.).

1. Expand the *Servers* folder in the Management Client's Site Navigation pane and select the *Recording Servers* node.
2. Right-click the no longer required recording server in the overview pane.
3. From the menu that appears, select *Remove Recording Server*.
4. You will be asked to confirm that you want to remove the recording server and all of its associated hardware from the RC-E system. If you are sure, click *Yes*.
5. The recording server and all of its associated hardware will be removed.

Replacing a Recording Server

If a recording server is malfunctioning and you want to replace it with a new server, while letting the new server inherit the settings of the old, malfunctioning recording server, do the following:

1. Retrieve the recording server ID from the old recording server;

a) In the Management Client's Site Navigation pane select *Recording Servers*, in the Overview pane select the old, required recording server.

b) In the Management Client's Properties pane, select the *Storage* tab.

c) Press and hold down the CTRL key on your keyboard while selecting the *Info* tab.

d) Copy the recording server ID found in the lower part of the *Info* tab. Do not copy *ID* = but only the ID itself.

IMPORTANT: Stop the Recording Server service (see "Management Server Service and Recording Server Service" on page 198) on the old recording server, then in Windows' *Services* set the service's *Startup type* to *Disabled.*

2. Replace recording server ID on the new recording server:

a) Make sure that the Recording Server service is stopped (see "Management Server Service and Recording Server Service" on page 198) and disabled on the old recording server.

It is very important that you do not start two recording servers with identical IDs at the same time.

b) On the new recording server, open an explorer and go to C:\ProgramData\OnSSI\OnSSI RC-E Recording Server or the path where your recording server is located.

c) Open the file *RecorderConfig.xml*.

d) Delete the ID stated in between the tags *<id>* and *</id>*.

e) Paste the copied recording server ID in between the tags *<id>* and *</id>*. Save the *RecorderConfig.xml* file.

f) Restart the recording server service. When the new Recording Server service starts up, the recording server has inherited all settings on the old recording server.

Tip: This procedure also applies if you re-install Windows on the computer running the recording server, even if you do not replace the computer running the recording server.

Troubleshooting: Missing Recording Servers

If you have installed several recording servers on your surveillance system, the recording servers should automatically be listed in the Management Client.

If your Management Client does not list all the recording servers you have installed, the most likely reason is that the missing recording servers have not been correctly configured to connect to a management server (in an RC-E system, recording servers point to management servers, not the other way round).

The configuration normally takes place during one of the steps in the recording server installation process. Here, you specified recording server setup parameters, among these the IP address or host name of the management server to which the recording server should be connected:

Fortunately, you do not have to re-install recording servers in order to specify which management servers they should connect to. Once a recording server is installed, you can verify/change its basic configuration the following way:

How to Verify/Change which Management Server a Recording Server Connects to:

In order to verify/change a recording server's basic configuration, the recording server service must be stopped. This means that recording and live viewing will not be possible while you verify/change the recording server's basic configuration.

1. On the computer running the recording server, right-click the recording server icon in the notification area:

   Tip: The notification area is occasionally also known as the system tray, it is located at the far right of the recording server computer's Windows taskbar.

2. From the menu that appears, select *Stop Recording Server Service*:

3. Right-click the notification area's *Recording Server* icon again.

4. From the menu that appears, select *Change Settings...*:

   The *Recording Server Settings* window appears. Verify/change the following settings:

   - ***Management server hostname/IP address:*** Lets you specify the IP address (example: *123.123.123.123*) or host name (example: ourserver) of the management server to which the recording server should be connected. This information is necessary in order for the recording server to be able to communicate with the management server.

   - ***Management server port:*** Lets you specify the port number to be used when communicating with the management server. Default is port 9993, although you are able to change this if required.

5. Click *OK*.

6. To start the Recording Server service again, right-click the notification area's *Recording Server* icon, and select *Start Recording Server Service*:

Failover Tab (Recording Server Properties)

A failover server is a spare recording server which can take over if a regular recording server becomes unavailable; see also About Failover Servers (see "Manage Failover Servers" on page 192).

If your organization uses failover servers, use the *Failover* tab to select which groups of failover servers should take over from a regular recording server if the recording server in question becomes unavailable.

To access the *Failover* tab, select the required recording server in the overview pane (see "Panes Overview" on page 36), then select the *Failover* tab in the properties pane (see "Panes Overview" on page 36).

Selecting Required Failover Groups

- **Benefits of Using Failover Groups**

  Grouping has a clear benefit: When you specify which failover servers should be able to take over from a recording server, you do not select a particular failover server; rather you select a failover group. If the selected group contains more than one failover server, this gives you the security of being able to have more than just one failover server ready to take over if the recording server becomes unavailable. For information about configuring failover groups, see Manage Failover Servers (on page 192).

- **Primary and Secondary Failover Group**

  For each recording server, you are able to select a primary and an optional secondary failover group. If the recording server becomes unavailable, a failover server from the primary failover group will take over. If you have also selected a secondary failover group, a failover server from the secondary group will take over in case all failover servers in the primary failover group are busy. This way, you only risk not having a failover solution in the rare case when all failover servers in the primary as well as in the secondary failover group are busy.

- How to Select Required Failover Groups

  1. Select the required failover group from the Primary failover group list.

  2. If you also want a secondary failover group for the recording server, repeat the process in the Secondary failover group list.

You cannot select the same failover group for use as both primary and secondary failover group.

Failover Service Communication Port

By default, TCP port 11000 is used for communication between recording servers and failover servers. Such communication is primarily about the configuration of the recording server from which the failover server should take over.

If required, you can change the port number. Note that if you change the port number, you must restart the Recording Server service (see "Management Server Service and Recording Server Service" on page 198) on the recording server in question.

Info Tab (Recording Server Properties)

You are able to verify or edit the name and description of a selected recording server on the *Info* tab. To access the *Info* tab, select the required recording server in the overview pane (see "Panes Overview" on page 36), then select the *Info* tab in the properties pane (see "Panes Overview" on page 36).

Info Tab's Fields

- ***Name***: Name of the recording server. The name will be used whenever the recording server is listed in RC-E and Ocularis Administrator. A name is not compulsory, but highly recommended. The name does not have to be unique.

  To change the name, simply overwrite the existing name and click *Save* in the toolbar (see "Management Client Overview" on page 34).

  Tip: If you change the name, it will be updated throughout RC-E. This means that if the name is used in, for example, a rule, the name will automatically change in the rule as well.

- ***Description***: Description of the recording server. The description will appear in a number of listings within RC-E. For example, the description will appear when pausing the mouse pointer over the recording server's name in the overview pane (see "Panes Overview" on page 36). A description is not compulsory.

  To specify a description, simply type the description and click *Save* in the toolbar (see "Management Client Overview" on page 34).

- ***Host name***: Non-editable field, displaying the recording server's host name.

- ***Web server URL***: Non-editable field, displaying the URL of the recording server's web server. The web server is used, for example, for handling PTZ camera control commands, and for handling browse and live requests from the Ocularis Client. The URL will include the port number used for web server communication (typically port 7563).

- ***Time zone:*** Non-editable field, displaying the time zone in which the recording server is located.

Storage Tab (Recording Server Properties)

On the *Storage* tab, you are able to setup, manage and view storage areas for selected recording servers. For a more general introduction to storing and archiving, see About Storage and Archiving (on page 56).

What is a storage area? A storage area is a directory in which database content— primarily recordings from the cameras connected to the recording server— is stored in at least a recording database and possibly archived in a number of archiving databases. A default storage area with a default recording database is automatically created for each recording server when the recording server is installed on the system. Unless you specifically define that another storage area should be used for particular cameras, recordings from connected cameras are stored in individual camera databases in the recording server's default storage area. Archives can be added to a storage area at any time convenient.

To access the *Storage* tab, select the required recording server on the Overview pane (see "Panes Overview" on page 36), then select the *Storage* tab in the Properties pane (see "Panes Overview" on page 36).

It is **not** possible to add databases or edit a storage area if the recording server is offline.

Storage Tab's Elements

Storage configuration list contents:

- *Name:* Indicates the name of the storage area. Click it to edit it.

- *Device Usage*: Indicates how many devises use the storage. Click the number link to see device details:

- *Default:* Indicates the default storage, i.e. the storage area in which database content is automatically stored unless you specifically define other storage areas for particular cameras. Only one storage at the time can be default.

Recording and archiving configuration list content:

1. Database name
2. Maximum size of the database (and usage; also represented graphically by a proportional filling of the database)
3. Database location
4. Archiving schedule for archiving to the next archive in the list. Note that the number of retention days stated for an archive includes all retention stated earlier in the process.

   Tip: Pausing the mouse pointer over a database will show detailed database information.

Creating a New Storage Area

A storage area is always created with at predefined recording database named *Recording,* which cannot be renamed. Besides a recording database, a storage area can contain a number of archives, see Creating an Archive within an Existing Storage Area (on page 67).

1. To add an extra storage area to a selected recording server, click the button located below the *Storage configuration* list.
2. This opens the *Storage and Recording Settings* dialog where you must specify the following:
   - ***Name:*** Rename the storage area if needed; use a descriptive and unique name.
   - **Path:** Type or use the browser link next to the field to specify the path to the directory in which to save the storage area. The storage area does not necessarily have to be located on the recording server computer itself.

     Tip: If the directory you plan to use does not already exist, you can create it using the browser dialog. Network drives must be specified using UNC (Universal Naming Convention) format, example: \\server\volume\directory\.
   - ***Retention time:*** Select a number of units and select either *Days* or *Hours* to specify how long recordings should stay in the recording database before being deleted or archived (depending on archive settings). This is useful if you do not want your most recent recordings to be archived (or deleted) straight away even though archiving may be scheduled to take place before the specified number of hours.

     Who determines the schedule? You do. You must specify the intervals with which the archiving process will start.

     Example: If you specify 24 hours, recordings must be at least a day old before they will be archived. If archiving is scheduled to take place before the 24 hours have passed, only recordings older than 24 hours will be archived. Bear in mind that the archive's scheduling may mean that recordings will be older than the specified number of hours before they are archived. This may especially be the case if you specify an archiving schedule with long time spans between archiving.

     Archiving is set up by adjusting several interdependent settings, see About Storage and Archiving (on page 56)for more information.
   - ***Maximum size:*** Select the maximum number of gigabytes of recording data to save in the recording database.

     Example: If you want to store up to 100 gigabytes of recording data in the database, select 100. Recording data in excess of the specified number of gigabytes will be auto-moved to the first archive in the list - if any is specified - or deleted.

IMPORTANT: This is one of two maximum size settings for the recording database. The *Retention Time* setting specified earlier may mean that recordings are removed from the recording database before the specified number of gigabytes is reached.

IMPORTANT: The oldest data in a database will always be auto-archived (or deleted if no next archive is defined) when less than 5GB of space is free. If less than 1GB space is free, data will be deleted. A database always requires 250MB of free space. If this limit is reached (if data is not deleted fast enough), no more data will be written to the database until enough space has been freed. The actual maximum size of your database will thus be the amount of gigabytes you specify, minus 5GB.

- ***Signing:*** Check this box if you want to write a digital signature to database files containing recorded data. This allows the Ocularis Client to verify that the contents of imported and opened databases have not been tampered with and that no database files have been removed.

  Note that signing is turned off per default as it may affect system performance.

- ***Encryption:*** Select the appropriate level of encryption for the recording database by selecting either *None*, *Light* or *Strong*.

  Note that the stronger the encryption, the more CPU usage it will cause.

- ***Password:*** (mandatory only if you selected *Light* or *Strong* in the *Encryption* field mentioned earlier)**:** Click *Set...* to set a password.

3. Click *OK*.

If needed, you are now ready to create archive(s) within your new storage area, see Creating an Archive within an Existing Storage Area (on page 67).

Creating an Archive within an Existing Storage Area

A storage area has no default archive when it is created.

1. To create an archive, select the wanted storage area by clicking it in the *Recording and archiving configuration* list.
2. Next, click the button located below the *Recording and archiving configuration* list.
3. This opens the *Archive Settings* dialog where you must specify the following:

   - ***Name:*** Rename if needed; use a descriptive and unique name.
   - ***Path:*** Type or use the browser link next to the field to specify the path to the directory in which to save the archive. The archive does not necessarily have to be located on the recording server computer itself.

     Tip: If the directory you plan to use does not already exist, you can create it using the browser dialog. Network drives must be specified using UNC (Universal Naming Convention) format, example: *server**volume**directory*\.

   - ***Retention time:*** Select a number of units and select either *Days* or *Hours* to specify how long recordings should stay in the archive before being moved to another archive or deleted (depending on archive settings). The retention time must always be longer than the retention time of the last archive or the recording database. This is due to the fact that the number of retention days stated for an archive includes all retention stated earlier in the process.

     Who determines the schedule? You do. You must specify the intervals with which the archiving process will start.

     Example: If you specify 24 hours, recordings must be at least a day old before they will be archived. If archiving is scheduled to take place before the 24 hours have passed, only recordings older than 24

hours will be archived. Bear in mind that the archive's scheduling may mean that recordings will be older than the specified number of hours before they are archived. This may especially be the case if you specify an archiving schedule with long time spans between archiving.

Archiving is set up by adjusting several interdependent settings, see About Storage and Archiving (on page 56)for more information.

- ***Maximum size:*** Select the maximum number of gigabytes of recording data to save in the archive.

  Example: If you want to store up to 100 gigabytes of recording data in the archive, select 100. Recording data in excess of the specified number of gigabytes will be auto-moved to the next archive in the list - if any is specified - or deleted.

  IMPORTANT: This is one of two maximum size settings for the storage area. The *Retention Time* setting specified earlier may mean that recordings are removed from the archive before the specified number of gigabytes is reached.

  IMPORTANT: The oldest data in a database will always be auto-archived (or deleted if no next archive is defined) when less than 5GB of space is free. If less than 1GB space is free, data will be deleted. A database always requires 250MB of free space. If this limit is reached (if data is not deleted fast enough), no more data will be written to the database until enough space has been freed. The actual maximum size of your database will thus be the amount of gigabytes you specify, minus 5GB.

- ***Schedule:*** Click the *Schedule* icon next to the *Schedule* field to specify an archiving schedule, i.e. the intervals with which the archiving process should start. If required, you are able to make archiving take place very frequently (in principle every minute all year round), or very infrequently (for example, every first Monday of every 36 months).

  What is the ideal interval? The ideal interval to use between each archiving process depends entirely upon your organization's needs. Consider your system's recording settings, make an estimate of the amount of data you expect to record within, for example, a day, a week, or a month, then decide on a suitable interval. Bear in mind that your organization's needs may change over time; it is thus a good idea to regularly monitor your archiving settings, and adjust them if required.

  In this example, we have selected that archiving should take place twice every week: at three o'clock in the morning on Wednesdays and Sundays. Note that regional settings on your computer may mean that dates and times appear differently in your version of RC-E.

  Tip: The effect of your selections is summed up in the lower part of the dialog. Use the summary to verify that your selections reflect your intentions.

  Tip: If required, you can always adjust the archive's settings—including its scheduling—once the archive has been created.

- ***Reduce frame rate:*** Select the *Reduce frame rate* check box and set a frame per second (FPS) in order to reduce FPS when archiving.

  Reducing frame rates by a selected number of FPS's will make your recordings take up less space in the archive. On the other hand, it also reduces quality since a number of frames are erased, leaving only FPS corresponding to the number of FPS selected in the dialog. MPEG/H.264 will be reduced to minimum key-frames.

  Tip: It is possible to reduce frame rates to less than 1 FPS, for example as low as 0.1 FPS which means 1 frame every 10 seconds.

4. Click *OK*.

Deleting an Archive from within an Existing Storage

1. To delete an archive, select the wanted archive from the *Recording and archiving configuration* list by clicking it. A selected archive is marked by a dark frame.

   It is only possible to delete the last archive in the list. The archive does not have to empty.

2. Click the button located below the *Recording and archiving configuration* list.

3. Click *Yes*.

Deleting an Entire Storage Area

Prerequisites

The storage area you want to delete must **not** be set as default storage area. Furthermore, it cannot be used by any devices to hold recordings. This means that you must possibly move devices and their **not yet archived** recordings to another storage area before you are allowed to delete the storage area, see Moving Non-archived Recordings from One Storage Area to Another (see "Moving Non-archived Recordings from One Storage to Another" on page 69).

To Delete an Entire Storage Area

1. To delete a storage area, select the wanted storage area by clicking it.

2. Click the button located below the *Storage configuration* list.

3. Click *Yes*.

Editing Settings for a Selected Storage Area or Archive

1. In the *Recording and archiving configuration* list, to edit a storage area, select its recording database. To edit an archive, select the archive database.

   Tip: A selected database is marked by a dark frame.

2. Click the button located below the *Recording and archiving configuration* list.

3. For editing a recording database, see Creating a New Storage Area (on page 66) and for editing an archive, see Creating a New Archive within an Existing Storage Area (see "Creating an Archive within an Existing Storage Area" on page 67).

If you change the maximum size of a database, recordings that exceed the new limit are auto-archived to the next archive or deleted - depending on archiving settings.

Moving Non-archived Recordings from One Storage to Another

1. Moving of contents from one recording database to another is done from the *Record* tab of the device in question.

2. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Devices,* select the wanted device type. In the Overview pane, select the wanted device.

3. In the Properties pane, click the *Record* tab. In the upper part of the *Storage* area, click *Select...* .

4. In the *Select Storage* dialog that follows, select the wanted database.

5. Click *OK*.
6. In the *Recordings Action* dialog that follows, select whether already existing - but **non-archived** -recordings should be moved along to the new storage or deleted.
7. After selecting, click *OK*.

See also Record Tab Overview (on page 103).

About Upgrading

If you upgrade your RC-E system to version 4.0 (or later), you might discover that you end up with a lot more storages than before the upgrade. This is due to the fact that from RC-E 4.0 and forward, the database structure is different than it used to be and during the update process, the system creates a number of extra databases. However, since your original naming-convention is respected, you are able to reconstruct your former database structure with only little modification of devices and deletion of obsolete storages or databases.

Manage Multicasting

OnSSI RC-E supports multicasting of live streams from recording servers. In cases when many Ocularis Client users want to view live video from the same camera, multicasting can help save considerable system resources.

Multicasting is only possible for live streams; not for recorded video/audio.

If a recording server has more than one network interface card, it is only possible to multicast on one of them. Through the Management Client you are able to specify which one to use.

The successful implementation of multicasting also requires that your network equipment (switches, etc.) has been set up to relay multicast data packets to the required group of recipients only. If not; multicasting may not be different from broadcasting, which can significantly slow down network communication.

What Is Multicasting?

In regular network communication, each data packet is sent from a single sender to a single recipient - a process known as unicasting. With multicasting, however, it is possible to send a single data packet (from a server) to multiple recipients (clients) within a group. Multicasting can thus help save bandwidth.

- When using **unicasting**, the source must transmit one data stream for each recipient.
- When using **multicasting**, only a single data stream is required on each network segment.

Multicasting is therefore an interesting option for streaming live video from recording servers to Ocularis Client s since video streams will not be duplicated on each network segment.

Multicasting as described here is **not** streaming of video from camera to servers.

With multicasting, you work with a clearly defined group of recipients, based on options such as IP address ranges, the ability to enable/disable multicast for individual cameras, the ability to define largest acceptable data packet size (MTU), the maximum number of routers a data packet must be forwarded between (TTL), etc. Thus, multicasting should not be confused with the much more primitive method *broadcasting*, which would send data to everyone connected to the network, even if the data is perhaps not relevant for everyone:

- *Unicasting* sends data from a single source to a single recipient
- *Multicasting* sends data from a single source to multiple recipients within a clearly defined group
- *Broadcasting* sends data from a single source to everyone on a network; broadcasting can thus significantly slow down network communication.

What Are the Requirements?

In order to use multicasting, your network infrastructure must support IGMP (Internet Group Management Protocol, an IP multicasting standard).

Furthermore, multicasting must be configured through the Management Client.

Enabling Multicasting

On the *Multicast* tab, select the *Live multicast* check box.

If the entire IP address range for multicast is already in use on one or more other recording servers, you cannot enable multicasting on further recording servers without freeing up some multicasting IP addresses first.

Assigning IP Address Range

In this section you specify the range from which you want to assign addresses for multicast streams from the selected recording server. Clients will connect to these addresses when viewing multicast video from the recording server in question.

- ***IP address:*** In the *Start* field, specify the first IP address in the required range. Then specify the last IP address in the range in the *End* field. For more info, see the following.
- ***Port***: In the *Start* field, specify the first port number in the required range. Then specify the last port number in the range in the *End* field.
- ***Source IP address for all multicast streams***: If a recording server has more than one network interface card, it is only possible to multicast on one of them. This field is therefore relevant if your recording server has more than one network interface card—or if it has a network interface card with more than one IP address.

  To use the recording server's default interface, leave the value 0.0.0.0 (IPv4) or :: (IPv6) in the field. If you want to use another network interface card, or a different IP address on the same network interface card, specify the IP address of the required interface.

Specifying Datagram Options

In this section you specify settings for data packets (datagrams) transmitted through multicasting.

- ***MTU***: Maximum Transmission Unit, the largest allowed physical data packet size (measured in bytes). Messages larger than the specified MTU will be split into smaller packets before being sent. Default value is 1500, which is also the default on most Windows computers and Ethernet networks.
- ***TTL***: Time To Live, the largest allowed number of hops a data packet should be able to travel before it is discarded or returned. A hop is a point between two network devices, typically a router. Default value is 128.

Enabling Multicasting for Individual Cameras

Even when you have specified multicasting settings for the selected recording server, multicasting will not work until you enable it for required cameras:

Select the required recording server in the Management Client's Site Navigation pane (see "Panes Overview" on page 36), select the required camera in the overview pane (see "Panes Overview" on page 36), then select *Live multicast* on the Client tab (see "Client Tab (Camera Properties)" on page 76) in the properties pane (see "Panes Overview" on page 36). Repeat for all required cameras under the recording server in question.

Specify IP Address Range

To specify the range from which you want to assign addresses for multicast streams from the selected recording server do the following:

For each multicast camera feed, the IP address/port combination (IPv4 example: 232.0.1.0:6000) must be unique. You can thus either use one IP address and many ports, or many IP addresses and fewer ports. By default, RC-E suggests a single IP address and a range of 1000 ports, but you can change this as required.

Example: If you want multicast for 1000 cameras, you would need either:

- 1 IP address and a range of 1000 different ports, OR
- a range of two IP addresses and a range of 500 different ports (or any matching combination), OR
- a range of 1000 IP addresses and a single port

When specifying the IP address, in the *Start* field, specify the first IP address in the required range. Then specify the last IP address in the range in the *End* field.

Tip: If required, a range may include only one IP address (IPv4 example: 232.0.1.0-232.0.1.0)

Tip: IP addresses for multicasting must be within a special range set aside for dynamic host allocation by IANA (the authority overseeing global IP address allocation). If using IPv4, you can read more about the range, which goes from 232.0.1.0 to 232.255.255.255, at www.iana.org/assignments/multicast-addresses (www.iana.org/assignments/ipv6-multicast-addresses). If using IPv6, the range is different; see www.iana.org/assignments/ipv6-multicast-addresses (www.iana.org/assignments/ipv6-multicast-addresses).

Manage Public Addresses

You define a recording server's public IP address on the *Network* tab. To access the *Network* tab, select the required recording server in the overview pane (see "Panes Overview" on page 36), then select the *Network* tab in the properties pane (see "Panes Overview" on page 36).

This description is also valid for failover servers (see "Manage Failover Servers" on page 192).

Why Use a Public Address?

When the Ocularis Client connects to a surveillance system, an amount of initial data communication, including the exchange of contact addresses goes on in the background. This happens automatically, and is completely transparent to users.

Ocularis Client users may connect from the local network as well as from the internet, and in each case the surveillance system should be able to provide suitable addresses so the clients can get access to live and recorded video from the recording servers:

- When clients connect locally, the surveillance system should reply with local addresses and port numbers. See also Manage Local IP Address Ranges (on page 171).
- When clients connect from the internet, the surveillance system should reply with the recording server's public address, i.e. the address of the firewall or NAT (Network Address Translation) router, and often also a different port number (which is then forwarded to recording servers).

  To provide access to the surveillance system from outside a NAT (Network Address Translation) firewall, RC-E lets you use public addresses and port forwarding. This will allow clients from outside the firewall to connect to recording servers without using VPN (Virtual Private Network). Each recording server (and failover server) can be mapped to a specific port and the port can be forwarded through the firewall to the server's internal address.

Enabling Public Access

To enable public access, select the *Network* tab's *Enable public* access box.

Defining Public Address and Port

When public access is enabled, you are able to define the recording server's public address and public port number in the *Public address* and *Public port* fields respectively.

As public address, use the address of the firewall or NAT router which clients accessing the surveillance system from the internet must go through in order to reach recording servers.

Specifying a public port number is compulsory; it is always a good idea that port numbers used on the firewall or NAT router are different from the ones used locally.

When using public access, the firewall or NAT router used must be configured so requests sent to the public address and port are forwarded to the local address and port of relevant recording servers.

Local IP Ranges

There are cases when the recording server's public address should not be used: When clients connect from the local network, the surveillance system should reply with local addresses and port numbers. The surveillance system must therefore be able to determine whether a client belongs on a local IP range or on the internet.

For this purpose, you are able to define a list of IP ranges which the surveillance system should recognize as coming from a local network. You do this by clicking *Configure...* on the *Network* tab. See Manage Local IP Address Ranges (on page 171) for more information.

Servers and Clients Require Time-Synchronization

Part of the security surrounding the use of remote clients with RC-E is based on time-based tokens.

Why Servers Require Time-Synchronization

When a client logs in to the surveillance system, the client receives a token from the management server. The token contains important security-related time information.

The management server also sends a similar token to the required recording server(s). This is partly due to the fact that recording servers may be located all around the world; each recording server thus uses the token to validate the client's token against the local time in the recording server's own time zone.

The validity of a token expires after a while. It is therefore important that time on your management server and all of your organization's recording servers is synchronized (minute and second-wise; hours may of course be different in different locations around the world). If time on the servers is not synchronized, you may experience that a recording server is ahead of the management server's time.

When a recording server is ahead of the management server's time, it may result in a client's token expiring on the recording server earlier than intended by the management server. Under unfortunate circumstances you might even experience that a recording server claims that a client's token has already expired when it receives it; effectively preventing the client from viewing recordings from the recording server.

How to synchronize time on your organization's servers depends on your network configuration, internet access, use of domain controllers, etc. Often, servers on a domain are already time-synchronized against the domain controller. If so, you should be fine as long as all required servers belong to the domain in question.

If your servers are not already time-synchronized, it will be necessary to synchronize the servers' time against a time server, preferably the same time server.

The following articles from Microsoft describe what to do in different situations:

- How to configure an authoritative time server in Windows Server 2003 (see http://support.microsoft.com/kb/816042/en-us - http://support.microsoft.com/kb/816042/en-us)
- Registry entries for the W32Time service (see http://support.microsoft.com/kb/223184/en-us - http://support.microsoft.com/kb/223184/en-us)

If these links do not work for you, try searching www.microsoft.com (see http://www.microsoft.com/ - http://www.microsoft.com/) for time server, time service, synchronize servers or similar.

It is also very important that Ocularis Client s are time-synchronized with the management server.

Why Clients Require Time-synchronization

Because configuration communication is facilitated by the Ocularis Base, Ocularis Client machines should also be time-synchronized with the management server and the Ocularis Base machine. A time difference of up to five minutes between Ocularis Client machines and servers is tolerated.

Devices

About Devices

To add cameras, go to Add Hardware (see "Add Hardware (Cameras, etc.)" on page 49). To replace cameras, go to Manage Hardware (on page 53).

In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), you are able to work with the following under *Devices*:

- ***Cameras***: (see "Manage Cameras" on page 75) Lets you handle the majority of camera configuration and management. ***Microphones*****:** (see "**Manage Microphones**" on page 85) On many devices you are able to attach external microphones; some devices even have built-in microphones.
- ***Speakers*** **:** (see "Manage Speakers" on page 87) On many devices you are able to attach external loudspeakers; some devices even have built-in speakers.
- ***Inputs*** **:** (see "Manage Input" on page 88) On many devices you are able to attach external units, typically external sensors, to input ports on the device. Input from such external input units can be used for many purposes in RC-E.
- ***Outputs*** **:** (see "Manage Output" on page 91) On many devices you are able to attach external units to output ports on the device. This allows you to activate/deactivate lights, sirens, etc. through RC-E.

Manage Cameras

To add cameras, go to Add Hardware (see "Add Hardware (Cameras, etc.)" on page 49). To replace cameras, go to Manage Hardware (on page 53).

Enabling/disabling as well as renaming of individual cameras takes place on the recording server hardware management level; see Managing Hardware (see "Manage Hardware" on page 53).

For all other configuration and management of cameras, expand *Devices* in the Management Client's Site Navigation pane (see "Panes Overview" on page 36), then select *Cameras*. In the overview pane (see "Panes Overview" on page 36), you group your cameras for an easy overview of your cameras. Grouping also lets you specify common properties for all cameras within a group in one step. See Using Device Groups (see "About Device Groups" on page 95) for information about creating groups as well as adding cameras to your groups.

Once you have placed your cameras in groups, configuration can begin.

Configuring Individual Cameras

You configure individual cameras by selecting the required camera in the list, then specifying the camera's required settings on the tabs in the *Properties* pane:

- The Info tab (see "Info Tab Overview" on page 101) for managing the selected camera's name, etc.
- The Settings tab (see "Settings Tab Overview" on page 106) for managing the selected camera's general settings.
- The Streams tab (see "About Multi-streaming" on page 98) for managing the selected camera's video streams.
- The Record tab (see "Record Tab Overview" on page 103) for managing the selected camera's recording, database and archiving storage settings.

- The Presets tab (see "PTZ Tab (Hardware Properties)" on page 102) for managing the selected camera's preset positions (only available if the selected camera is a PTZ camera).
- The Patrolling tab (see "PTZ Patrolling Tab (Camera Properties)" on page 80) for managing the selected camera's patrolling profiles (only available if the selected camera is a PTZ camera).
- The Events tab (see "Events Tab Overview" on page 99) for managing hardware configurable events.
- The Client tab (see "Client Tab (Camera Properties)" on page 76) lets you specify information which will affect client's use of the selected camera.
- The Privacy Mask tab (see "Privacy Mask Tab (Camera Properties)" on page 79) lets you enable and configure privacy masking for the selected camera.
- The Motion tab (see "Motion Tab (Camera Properties)" on page 77) for managing the selected camera's motion detection settings.

Client Tab (Camera Properties)

The *Client* tab lets you specify information which will affect clients' use of the selected camera. To access the *Client* tab, select the required camera in the overview pane (see "Panes Overview" on page 36), then select the *Client* tab in the properties pane (see "Panes Overview" on page 36).

Client Settings

- ***Live multicast*:** RC-E supports multicasting (see "Manage Multicasting" on page 70) (sending of single data packets to multiple recipients within a group, thereby saving bandwidth and system resources) of live streams from recording servers to Ocularis Client s. To enable multicasting of live streams from the selected camera, select the check box.

  Remember that for the feature to work, multicasting must also be configured for the recording server; see Manage Multicasting (on page 70). If multicasting is not possible, for example due to restrictions on the network or on individual clients, RC-E will revert to unicasting (sending of separate data packets to separates recipients).

- ***Default microphone*:** By defining a default microphone, you can determine from which microphone Ocularis Client users should by default hear recordings when they select the camera in question in their Ocularis Client s. The users can subsequently select another microphone if they require so**.**

  Bear in mind that although you have defined a default microphone for a camera, it cannot be guaranteed that all Ocularis Client users will hear audio from the microphone in question: Some users may not have speakers attached, some users may not have the rights required to listen to audio, etc.

- ***Default Speaker*:** By defining a default speaker, you can determine through which microphone Ocularis Client users should by default be able to speak when they select the camera in question in their Ocularis Client s. The users can subsequently select another speaker if they require so.

  Bear in mind that although you have defined a default speaker for a camera, it cannot be guaranteed that all Ocularis Client users will be able to talk through the speaker in question: Some users may not have a microphone attached, some users may not have the rights required to talk through speakers, etc.

- ***Shortcut***: Users of the Ocularis Client can take advantage of a range of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers, which are used to identify each camera. In the Management Client, each camera's shortcut number is specified in the **Shortcut** field.

  A camera shortcut number must not contain any letters or special characters, and cannot be longer than four digits. Examples of correct camera shortcut numbers: *3*, *1234*. Examples of incorrect camera shortcut numbers: *A*3*, *12345*. Always use a unique camera shortcut number for each camera.

Tip: Find more information about audio and keyboard shortcuts from a Ocularis Client user's perspective in the separate Ocularis Client documentation available from www.onssi.com.

Motion Tab (Camera Properties)

The *Motion* tab lets you enable and configure motion detection for the selected camera. Motion detection configuration is a key element in your RC-E surveillance solution: Your motion detection configuration may determine when video is recorded, when events are generated, when external output (such as lights or sirens) is triggered, etc.

Time spent on finding the best possible motion detection configuration for each camera may therefore help you later avoid unnecessary alarms, etc. Depending on the physical location of the camera, it may be a very good idea to test motion detection settings under different physical conditions (day/night, windy/calm weather, etc.).

Before you configure motion detection for a camera, it is highly recommended that you have configured the camera's image quality settings, such as resolution, compression, etc., on the *Settings* tab (see "Settings Tab Overview" on page 106). If you later change image quality settings, you should always test any motion detection configuration afterwards.

Tip: You can configure motion detection for all cameras in a device group (see Manage Cameras (on page 75)) in one step. Note, however, that some motion detection settings must be configured individually for each camera. This is the case with exclude regions (areas in which not to use motion detection), as these are very likely to vary from camera to camera.

Enabling and Disabling Motion Detection

Motion detection is enabled by default. To enable/disable motion detection for a camera, select/clear the *Motion* tab's *Motion detection* check box.

When motion detection is disabled for a camera, any motion detection-related rules (see "Manage Rules" on page 133) for the camera will not work.

Motion Detection Settings

You are able to specify settings relating to the amount of change required in a camera's video in order for the change to be regarded as motion. You are also able to specify intervals between motion detection analyses, any areas of an image in which motion should be ignored, etc.

Sensitivity Slider:

The *Sensitivity* slider determines **how much each pixel** in the camera's images must change before it is regarded as motion.

Drag the slider to the left for a higher sensitivity level, and to the right for a lower sensitivity level.

The *higher* the sensitivity level, the less change will be allowed in each pixel before it is regarded as motion.

The *lower* the sensitivity level, the more change in each pixel will be allowed before it is regarded as motion. This way you are able to allow insignificant changes, which should not be regarded as motion.

Pixels in which motion is detected are highlighted in green in the preview image. Select a slider position in which only detections you consider motion are highlighted.

Tip: Your exact sensitivity slider setting is indicated by a number from 0-300 in the right side of the slider. This way you are able to compare the exact sensitivity slider setting between cameras.

Tip: If you find the concept of motion detection sensitivity difficult to grasp, try dragging the slider to the left towards the highest possible sensitivity (0) position: The more you drag the slider towards the highest possible sensitivity position, the more of the preview image becomes highlighted in green. This is because with a very high sensitivity level even the slightest change in each pixel will be regarded as motion.

Motion Slider:

The *Motion* slider determines **how many pixels** in the camera's images image must change before it is regarded as motion.

The selected motion level is indicated by the black vertical line in the motion indication bar above the sliders.

The black vertical line in the motion indication serves as a threshold: When detected motion is above the selected sensitivity level, the bar changes color from green to red, indicating a positive detection.

Tip: Your exact motion slider setting is indicated by a number from 0-10.000 in the right side of the slider. This way you are able to compare the exact motion slider setting between cameras.

Keyframes Settings:

A keyframe is a single frame stored at specified intervals. The keyframe contains the entire view of the camera, whereas the following frames contain only the pixels that change. This helps greatly reduce the size of files.

If the check box is not available, or not selected, every frame will contain the entire view of the camera.

Image Processing Interval:

You are able to select how often motion detection analysis should be carried out on video from the camera.

From the *Process image every (msec):* list, select the required interval: every 100 milliseconds (i.e. once every tenth of a second), every 250 milliseconds, every 500 milliseconds, every 750 milliseconds, or every 1000 milliseconds (i.e. once every second). Default is every 500 milliseconds.

The interval is applied regardless of the camera's frame rate settings.

Detection Method:

You are able to optimize motion detection performance by analyzing only a selected percentage of the image, for example 25%. By analyzing 25%, only every fourth pixel in the image is analyzed instead of all pixels.

Using optimized detection will reduce the amount of processing power used to carry out the analysis, but will also mean a less accurate motion detection.

In the *Detection method* drop down-box, select the wanted detection method.

Ignoring Motion Detection in Parts of Images:

The *Exclude Regions* settings in the lower part of the *Motion* tab lets you disable motion detection in specific areas of a camera's images. Parts of images in which motion should be ignored this way are called *exclude regions*.

Disabling motion detection in specific areas may help you avoid detection of irrelevant motion, for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background.

When exclude regions are used with PTZ cameras and you pan/tilt/zoom the camera, the excluded area will not move accordingly. This might mean that objects originally excluded will be included. This is due to the fact that the exclude region is locked according to the camera's view, not the excluded region.
Consequently, it is not recommended to use exclude regions with PTZ cameras.

To use exclude regions, select the *Use exclude regions* check box.

Defining Exclude Regions:

When you select the *Use Exclude regions* check box, the preview image will be divided into selectable sections by a grid.

To define exclude regions, drag the mouse pointer over the required areas in the preview image. Pressing down the left mouse button selects a grid section; right mouse button clears a grid section.

You are able to define as many exclude regions as you require. Excluded regions are shown in blue.

The blue exclude area indications will only appear in the preview image on the *Motion* tab, not in any other preview images in the Management Client or access clients.

- ***Grid Size***
  The value selected in the *Grid size* list determines the density of the grid, regardless whether the grid is shown or not.

Select between the values 8×8 (i.e. a grid dividing the image into eight sections along the X-axis and eight sections along the Y-axis), 16×16, 32×32 or 64×64.

With a grid of 8×8, the image will be divided into relatively few sections for you to select for exclude regions. Each section will be relatively large; you will not be able to define very detailed exclude regions. With a grid size of 64×64, the image will be divided into relatively many sections for you to select for exclude regions. Each section will be relatively small, enabling you to define more detailed exclude regions.

- ***Show Grid***
  The grid may be visible or hidden, depending on whether the *Show grid* check box is selected or not.

  When the *Show grid* check box is selected (default), the preview image will feature a grid indicating the division of the preview image into selectable sections. The grid may help you when selecting exclude regions in the preview image.

  The density of the grid is determined by the value selected in the *Grid size* list.

  Showing the grid is not a requirement for selecting exclude regions; even without the grid you are able to select exclude regions as described earlier. Hiding the grid may provide a less obscured view of the preview image.

- ***Show Regions***
  When the *Show regions* check box is selected (default), exclude regions will be highlighted in blue in the preview image.

  Hiding exclude regions may provide a less obscured view of the preview image. However, under normal circumstances it is highly recommended that you keep the *Show regions* box selected; otherwise exclude regions may exist without you or your colleagues being aware of it.

  The blue exclude area indications will only appear in the preview image on the *Motion* tab, not in any other preview images in the Management Client or access clients.

- ***Pen size***
  Use the *Pen size* slider to indicate the size of the selections you wish to make when clicking and dragging the grid to select regions for privacy masking. Default is set to small, which is equivalent to one square in the grid.

Privacy Mask Tab (Camera Properties)

The *Privacy Mask* tab lets you enable and configure privacy masking for the selected camera. Among other things, you can define if and how selected areas of a camera's view should be masked before distribution. For example, if a surveillance camera films a street, in order to protect residents privacy, you can mask certain areas of a building (could be windows and doors) with privacy masking. This is required in some countries to comply with national legislation.

As Administrator you are also able to see through privacy masked areas, and can turn showing of privacy masked areas on and off. When viewed via Ocularis Client, privacy masked areas will be represented as black areas and it is impossible to see behind the privacy masking or in any way remove it.

When privacy masks are used with PTZ cameras and you pan/tilt/zoom the camera, the selected area masked for privacy will **not** move accordingly. This might mean that objects masked for privacy become visible. This is due to the fact that the masked area is locked according to the camera's view, not the masked object. Consequently, it is not recommended to use privacy masking with PTZ cameras.

Enabling and Disabling Privacy Masking

The privacy masking feature is enabled by default. To enable/disable the privacy masking feature for a camera, select/clear the *Privacy Mask* tab's *Privacy masking* check box.

Privacy Masking Settings

When you enable privacy masking, the preview image is divided into selectable sections by a grid.

To define privacy mask regions, drag the mouse pointer over the required areas in the preview image. Pressing down left mouse button selects a grid section; right mouse button clears a grid section.

You are able to define as many privacy mask regions as you require. Privacy mask regions are shown in red.

The red privacy mask indications will also appear in the preview image on the *Motion* tab.

- **Grid Size**
  The value selected in the *Grid size* list determines the density of the grid, regardless whether the grid is shown or not.

  Select between the values 8×8 (i.e. a grid dividing the image into eight sections along the X-axis and eight sections along the Y-axis), 16×16, 32×32 or 64×64.

  With a grid of 8×8, the image will be divided into relatively few sections for you to select for privacy mask regions. Each section will be relatively large; you will not be able to define very detailed privacy mask regions. With a grid size of 64×64, the image will be divided into relatively many sections for you to select for privacy mask regions. Each section will be relatively small, enabling you to define more detailed privacy mask regions.

- **Show Grid**

  The grid may be visible or hidden, depending on whether the *Show grid* check box is selected or not.

  When the *Show grid* check box is selected (default), the preview image will feature a grid indicating the division of the preview image into selectable sections. The grid may help you when selecting privacy mask regions in the preview image.

  Showing the grid is not a requirement for selecting privacy mask regions; even without the grid you are able to select privacy mask regions as described above. Hiding the grid may provide a less obscured view of the preview image.

- **Show Privacy Masks**

  When the *Show privacy masks* check box is selected (default), privacy mask regions will be highlighted in red in the preview image.

  Hiding privacy mask regions may provide a less obscured view of the preview image.

  However, under normal circumstances it is highly recommended that you keep the *Show privacy masks* box selected; otherwise exclude privacy mask regions may exist without you or your colleagues being aware of it.

- **Pen size**

  Use the *Pen size* slider to indicate the size of the selections you wish to make when clicking and dragging the grid to select regions for privacy masking. Default is set to small, which is equivalent to one square in the grid.

PTZ Patrolling Tab (Camera Properties)

The *Patrolling* tab lets you create patrolling profiles, the automatic movement of a PTZ (Pan/Tilt/Zoom) camera between a number of preset positions (see "PTZ Presets Tab (Camera Properties)" on page 83). Before you are able to work with patrolling, you must have specified at least two preset positions for the camera.

You manage patrolling on the *Patrolling* tab, which is available only when the selected camera is a PTZ camera.

Patrolling profiles are the definitions of how patrolling should take place. This includes the order in which the camera should move between preset positions, how long it should remain at each position for, etc. You are able to create an unlimited number of such patrolling profiles and use them in your rules (see "Manage Rules" on page 133). For

example, you may create a rule specifying that one patrolling profile should be used during daytime opening hours, and another during nights.

In order to use PTZ cameras' features, including the ability to pan, tilt, and zoom, operators must have a role which gives them the necessary rights. See About Roles (on page 145) for more information, including step-by-step descriptions of how to assign users to roles and how to specify the rights of roles.

Adding a New Patrolling Profile

1. Click *New*. This will open the *Add Profile* dialog.
2. In the *Add Profile* dialog, specify a name for the patrolling profile:

   Tip: Use a descriptive name; the name of the patrolling profile may later be used in situations where you will not have access to details about the patrolling profile, e.g. when using the patrolling profile in a rule (see "Manage Rules" on page 133).
3. Click *OK*. The new patrolling profile will be added to the *Patrolling* tab's *Profile* list. You are now able to specify required preset positions and other settings for the patrolling profile.

Specifying Preset Positions for Use in a Patrolling Profile

1. Select the required patrolling profile in the *Profile* list:
2. Click *Add* . This will open the *Select Preset* dialog.
3. In the *Select Preset* dialog, select the preset positions required for your patrolling profile:
4. Click *OK*. The selected preset positions are added to the list of preset positions for the patrolling profile:
5. The preset position at the top of the list will be used as the first stop when the camera patrols according to the patrolling profile, the preset position in second position from the top will be the second stop, and so forth.

   If required, change the sequence by selecting the required preset position and using the up/down buttons:

   Tip: If required, you can easily add more preset positions to the list by clicking *Add* , or remove unwanted preset positions from the list by selecting the unwanted preset position, then clicking *Remove*.

Specifying How Long to Stay at Each Preset Position

When patrolling, the PTZ camera will by default remain for 5 seconds at each preset position specified in the patrolling profile before it moves on to the next preset position. To change the number of seconds for which the PTZ camera will remain at a specific preset position, do the following:

1. Select the required patrolling profile in the *Profile* list.
2. In the list of preset positions for the selected patrolling profile, select the preset position for which you want to change the time:
3. Specify the required time (in number of seconds) in the *Wait time (secs.)* field:
4. If required, repeat for other preset positions.

Customizing Transitions

By default, the time required for moving the camera from one preset position to another, known as *transition*, is estimated to be 3 seconds. During this time, motion detection is by default disabled on the camera, as irrelevant motion is otherwise likely to be detected while the camera moves between the preset positions. Transitions are also known as PTZ scanning.

Customizing speed for transitions is only supported if your camera supports PTZ scanning and is of the type where preset positions are configured and stored on the RC-E server (type 1 PTZ camera). Otherwise the *Speed* slider is grayed out.

You can customize the transitions between each of the preset positions in a patrolling profile. You are able to customize the following:

- The estimated transition time
- The speed with which the camera will move during a transition
- Which plug-ins to disable during transition.

To customize transitions between preset positions in a patrolling profile, do the following:

1. Select the required patrolling profile in the *Profile* list.
2. Select the *Customize transitions* check box:

   This will add transition indications to the list of preset positions for the selected patrolling profile.
3. In the list, select the required transition:
4. Specify the estimated transition time (in number of seconds) in the *Expected time (secs.)* field:
5. Use the *Speed* slider to specify the required transition speed. When the slider is in its rightmost position, the camera will move with its default speed. The more you move the slider to the left, the slower the camera will move during the selected transition.

   Tip: A number indicating the exact speed is displayed near the top right corner of the slider. When required, the number (from 0.0001 (very slow) to 1.0000 (default speed)) allows you to define exactly the same custom speed across transitions.
6. In the *Plug-ins to disable* list, specify any plug-ins you want to disable during the selected transition. By default, the plug-in used for motion detection on the camera (*MotionDetectionPlugin*) is disabled in order to avoid irrelevant motion being detected during transition.

   To add a plug-in to the list, click *Add...*, and select the required plug-in. This requires that one or more other plug-ins are available, and that they can be disabled.

   To remove a plug-in from the list, for example if you do not want motion detection to be disabled during the transition, select the plug-in and click *remove*.
7. Repeat as required for other transitions.

Specifying an End Position

You are able to specify that the camera should move to a specific preset position when patrolling according to the selected patrolling profile ends.

1. Select the required patrolling profile in the *Profile* list.
2. Select the *Go to specific preset on finish* check box:

   This will open the *Select Preset* dialog.
3. In the *Select Preset* dialog, select the required end position, and click *OK*.

   Tip: You can select any of the camera's preset positions as the end position, you are not limited to the preset positions used in the patrolling profile.

4. The selected end position is added to the list of preset positions for the selected patrolling profile. When patrolling according to the selected patrolling profile ends, the camera will go to the specified end position.

Renaming an Existing Patrolling Profile

1. Select the required patrolling profile in the *Profile* list.
2. Click *Rename*. This will open the *Rename Profile* dialog.
3. In the *Rename Profile* dialog, type a new name for the patrolling profile.

   Tip: Use a descriptive name; the name of the patrolling profile may later be used in situations where you will not have access to details about the patrolling profile, e.g. when using the patrolling profile in a rule (see "Manage Rules" on page 133).
4. Click *OK*.

Specifying Manual PTZ Session Timeout

Patrolling of PTZ cameras may be interrupted manually by Ocularis Client users with the necessary user rights.

You are able to specify how much time should pass before regular patrolling is resumed after a manual interruption:

1. In the Management Client's menu bar, select *Tools* > *Options*. This will open the *Options* window.
2. On the *Options* window's *General* tab, select the required amount of time in the *PTZ manual session timeout* list (default is 15 seconds).

The setting will apply for all PTZ cameras on your RC-E system.

PTZ Presets Tab (Camera Properties)

The *Presets* tab lets you create preset positions to be used, for example, in rules (see "Manage Rules" on page 133) for making a PTZ (Pan/Tilt/Zoom) camera move to a specific preset position when an event occurs, as well as in patrolling (see "PTZ Patrolling Tab (Camera Properties)" on page 80), the automatic movement of a PTZ camera between a number of preset positions.

You manage preset positions on the *Presets* tab, which is available only when the selected camera is a PTZ (Pan/Tilt/Zoom) camera. The *Presets* tab will not be available if the selected PTZ camera does not support preset positions.

In order to use PTZ cameras' features, including the ability to pan, tilt, and zoom, operators must have a role which gives them the necessary rights. See About Roles (on page 145) for more information, including step-by-step descriptions of how to assign users to roles and how to specify the rights of roles.

Adding a Preset Position

As an alternative to defining preset positions in RC-E, preset positions may for some PTZ cameras also be defined on the camera device itself (typically by accessing a device-specific configuration web page) and imported into RC-E by selecting *Use presets from device*.

To add a preset position for the camera in RC-E, do the following:

1. Click *Add...*. This will open the *Add Preset* window:
2. The *Add Preset* window displays a preview image from the camera; use the navigation buttons and/or sliders to move the camera to the required preset position. While you do this, you are able to verify the position of the camera through the preview image.
3. Specify a name or number for the preset position in the *Name* field.

Tip: If typing a name, use a descriptive name; the name of the preset position may later be used in situations where you will not have access to a preview image from the preset position, e.g. when using the preset in a rule (see "Manage Rules" on page 133).

4. Optionally, type a description of the preset position in the *Description* field.
5. Click *OK*. This will close the *Add Preset* window, and add the preset position to the *Presets* tab's list of available preset positions for the camera.

How to Use the Axes Navigation Sliders

The navigation sliders let you to move the camera along each of its axes. Click inside the sliders to move the sliders' red handles to the required positions.

The slider for the ***X-axis*** (allowing you to pan left/right) is located immediately below the preview image.

The slider for the ***Y-axis*** (allowing you to tilt the camera up/down) is located immediately to the left of the preview image.

The slider for the ***Z-axis*** (allowing you to zoom in and out) is located immediately above the preview image. The camera will zoom in when you move the slider towards *Tele*, and zoom out when you move the slider towards *Wide*.

How to Use the Iris Slider

Iris settings are only available for some cameras.

Iris settings control the amount of light in images. The higher the iris setting, the lighter images will appear.

Click inside the slider to move the slider's red handle to the required position.

How to Use the Focus Slider

Focus settings are only available for some cameras.

Click inside the slider to move the slider's red handle to the required position.

Using Preset Positions from Device

As an alternative to specifying preset positions in RC-E, preset positions may for some PTZ cameras also be defined on the camera device itself (typically by accessing a device-specific configuration web page.

Such device-defined presets can subsequently be imported into RC-E by selecting *Use presets from device*.

If importing presets from the camera device, any presets you have previously defined for the camera in RC-E will be removed; this will affect any patrolling profiles in which these presets are used, as well as any rules in which the affected patrolling profiles are used.

If you later wish to edit such device-defined presets, editing should take place on the camera device.

Assigning a Default Preset Position

If required, you are able to assign one of a PTZ camera's preset positions at the camera's default preset position.

Having a default preset position can be useful because it allows you to define rules (see "Manage Rules" on page 133) specifying that the PTZ camera should go to the default preset position under particular circumstances, for example after the PTZ camera has been operated manually.

To assign a preset position as the default, select the required preset in your list of defined preset positions, then select the *default preset* box below the list.

Only one preset position can be the default preset position.

Editing a Preset Position

To edit an existing preset position defined in RC-E (presets imported from a device should be edited on the device itself), do the following:

1. Select the required preset position in the *Presets* tab's list of available preset positions for the camera.
2. Click *Edit...*. This will open the *Edit Preset* window:
3. The *Edit Preset* window displays a preview image from the preset position in question; use the navigation buttons and/or sliders to change the preset position as required.
4. Change the name/number and description of the preset position as required.

   Tip: If using a name, make sure it is descriptive; the name of the preset position may later be used in situations where you will not have access to a preview image from the preset position, e.g. when using the preset in a rule (see "Manage Rules" on page 133).
5. Click *OK*.

Testing a Preset Position

1. Select the required preset position in the *Presets* tab's list of available preset positions for the camera.
2. Click *Test*.
3. The *Presets* tab's preview image will move to the selected preset position.

   Tip: If the preview image does not appear to move to the selected preset position when you click *Test*, verify that preview image does not already show the selected preset position. In that case, try testing another preset position first.

360 Degree Lens Tab (Camera Properties)

Use of 360° technology requires a dedicated ImmerVision 360° lens mounted.

In this way, 360° technology enables panomorph technology through an advanced lens.

The *360° Lens* tab lets you enable and configure panomorph support for the selected camera.

Enabling and Disabling Panomorph Support

The panomorph feature is disabled by default.

To enable/disable it, select/clear the *360° Lens* tab's *Enable panomorph support* check box.

Panomorph Settings

When enabling the panomorph support functionality, you must also select a Registered Panomorph Lens (RPL) number from the *ImmerVision Enables® panomorph RPL number* list. This is to ensure identification and correct configuration of the lens used with the camera in question. The RPL number is usually found on the lens itself or on the box it came in. For details of ImmerVison, panomorph lenses, and RPLs, see http://www.immervision.com/en/home/index.php **(see http://www.immervision.com/en/home/index.php -** http://www.immervision.com/en/home/index.php**).**

You must also indicate the physical position/orientation of the camera in question. This is done by selecting its position from the *Camera position/orientation* list.

Manage Microphones

On many devices you are able to attach external microphones; some devices even have built-in microphones.

Devices' microphones are automatically detected when you add the devices to your RC-E system through the Management Client's *Add Hardware* (see "*Add Hardware (Cameras, etc.)*" on page 49) wizard, regardless of which of the wizard's detection options you use.

Microphones do not require separate licenses; you can use as many microphones as required on your system.

You can use microphones completely independently of cameras.

Who is able to listen to audio recorded by microphones? Users of the Ocularis Client can—provided microphones are available, and the users have the rights to use them—listen to audio from microphones. Roles (see "About Roles" on page 145) determine users' right to listen to microphones. You cannot listen to microphones from the Management Client.

Tip: RC-E comes with a default rule (see "Manage Rules" on page 133) which ensures that audio feeds from all connected microphones and speakers are automatically fed to the RC-E system. Like other rules, the default rule can be deactivated and/or modified as required.

You have two entry points for managing microphones:

- In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Devices*, select *Microphones*, expand the required device group, and select the required microphone. If no device groups are available, you must first group your microphones: See Using Device Groups (see "About Device Groups" on page 95) for information about creating groups as well as adding microphones to your groups.

- In the Management Client's Site Navigation pane, expand *Servers* and select *Recording Servers*, then in the overview pane (see "Panes Overview" on page 36) expand the required recording server, expand the required device and select the required microphone.

Check the RC-E release notes to verify that microphones are supported for the devices and firmware used.

Enabling Microphones

When microphones are detected with the wizard *Add Hardware* (see "*Add Hardware (Cameras, etc.)*" on page 49) they are by default disabled. You can enable microphones when needed. If a device has several microphones you can enable one, some, or all of them as required.

1. In the Site Navigation pane (see "Panes Overview" on page 36), expand *Servers* and select *Recording Servers*.

2. In the Overview pane (see "Panes Overview" on page 36), expand the relevant recording server, and find the device on which the microphone is placed.

3. Right-click the required microphone, and select *Enabled*.

On some devices, a microphone can also be enabled/disabled on the device itself, typically through the device's own configuration web page. If a microphone does not work after enabling it in the Management Client, you should thus verify whether the problem may be due to the microphone being disabled on the device itself.

Configuring Individual Microphones

You configure individual microphones by selecting the required microphone in the list, then specifying the microphone's required settings on the tabs in the Properties pane (see "Panes Overview" on page 36):

- The *Info* tab (see "Info Tab Overview" on page 101) for managing the selected microphone's name, etc.

- The *Settings* tab (see "Settings Tab Overview" on page 106) for managing the selected microphone's general settings.

- The *Record* tab (see "Record Tab Overview" on page 103) for managing the selected microphone's recording, database and archiving storage settings.

- The *Events* tab (see "Events Tab Overview" on page 99) for managing hardware configurable events.

Viewing Current State of a Microphone

When you have selected a microphone in the Management Client, information about the current status of the selected microphone is presented in the preview pane (see "Panes Overview" on page 36).

Manage Speakers

On many devices you are able to attach external loudspeakers; some devices even have built-in speakers.

Devices' speakers are automatically detected when you add the devices to your RC-E system through the Management Client's *Add Hardware* (see "*Add Hardware (Cameras, etc.)*" on page 49) wizard, regardless of which of the wizard's detection options you use. Speakers do not require separate licenses; you can use as many speakers as required on your system.

You can use speakers completely independently of cameras.

Who is able to talk through speakers? Users of the Ocularis Client can—provided speakers are available, and the users have the rights to use them—click a button to talk through speakers. Roles (see "Manage Roles" on page 147) determine users' right to talk through speakers. You cannot talk through speakers from the Management Client.

What happens if two users want to speak at the same time? Roles determine users' right to talk through speakers. As part of the roles definition, you are able to specify a speaker priority from very high to very low. If two users want to speak at the same time, the user whose role has the highest priority will win the ability to speak. If two users with the same role want to speak at the same time, the first-come first-served principle applies.

Tip: RC-E comes with a default rule (see "Manage Rules" on page 133) which ensures that audio feeds from all connected microphones and speakers are automatically fed to the RC-E system. Like other rules, the default rule can be deactivated and/or modified as required.

You have two entry points for managing speakers:

- In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Devices*, select *Speakers*, expand the required device group, and select the required speaker. If no device groups are available, you must first group your speakers: See About Device Groups (on page 95) for information about creating groups as well as adding speakers to your groups.
- In the Management Client's Site Navigation pane, expand *Servers* and select *Recording Servers.* In the overview pane (see "Panes Overview" on page 36), expand the required recording server and select the required speaker.

Check the RC-E release notes to verify that speakers are supported for the devices and firmware used.

Enabling Speakers

When speakers are detected with the wizard *Add Hardware*, they are by default disabled. You can enable speakers when needed. If a device has several speakers you can enable one, some, or all of them as required.

1. In the Site Navigation pane (see "Panes Overview" on page 36), expand *Servers* and select *Recording Servers*.
2. In the Overview pane (see "Panes Overview" on page 36), expand the relevant recording server, and find the device on which the speaker is placed.
3. Right-click the required speaker, and select *Enabled*.

On some devices, a speaker can also be enabled/disabled on the device itself, typically through the device's own configuration web page. If a speaker does not work after enabling it in the Management Client, you should thus verify whether the problem may be due to the speaker being disabled on the device itself.

Configuring a Speaker

You configure individual speakers by selecting the required speaker in the list, then specifying the speaker's required settings on the tabs in the Properties pane:

1. The *Info* tab (see "Info Tab Overview" on page 101) for managing the selected speaker's name, etc.
2. The *Settings* tab (see "Settings Tab Overview" on page 106) for managing the selected speaker's general settings.
3. The *Record* tab (see "Record Tab Overview" on page 103) for managing the selected speaker's recording, database and archiving storage settings.

Viewing Current State of a Speaker

When you have selected a speaker in the Management Client, information about the current status of the selected speaker is presented in the preview pane.

Manage Input

On many devices you are able to attach external units to input ports on the device. Input units are typically external sensors. Such external sensors may, for example, be used for detecting if doors, windows, or gates are opened. Input from such external input units is treated as events by RC-E.

Such events can be used in rules (see "Manage Rules" on page 133). For example, you could create a rule specifying that a camera should begin recording when an input is activated, and stop recording 30 seconds after the input is deactivated.

Devices' input ports are automatically detected when you add the devices to your RC-E system through the Management Client's Add Hardware (see "Add Hardware (Cameras, etc.)" on page 49) wizard, regardless of which of the wizard's detection options you use.

You have two entry points for managing input:

- In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Devices*, select *Inputs*, expand the required device group, and select the required input. If no device groups are available, you must first group your input: See About Device Groups (on page 95) for information about creating groups as well as adding input to your groups.
- In the Management Client's Site Navigation pane, expand *Servers* and select the *Recording Server* node, then expand the required recording server in the overview pane (see "Panes Overview" on page 36) and select the required input.

Before you specify use of external input and output units on a device, verify that sensor operation is recognized by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the RC-E release notes to verify that input- and output-controlled operations are supported for the devices and firmware used.

Enabling Input

When inputs are detected with the *Add Hardware* (see "*Add Hardware (Cameras, etc.)*" on page 49) process, they are by default disabled. You can activate inputs when needed. If a device has several inputs you can enable one, some, or all of them as required.

1. In the Site Navigation pane (see "Panes Overview" on page 36), expand *Servers* and select *Recording Servers.*
2. In the Overview pane (see "Panes Overview" on page 36) expand the relevant recording server, and find the device on which the input is placed.

3. Right-click the required input, and select *Enabled*.

Specifying Input Properties

Each input typically has several properties. You can access these properties in two ways:

- In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Devices,* and select *Inputs*. In the Overview pane expand the required inputs folder and select the required input.

  - or -

- In the Overview pane (see "Panes Overview" on page 36), select a device group to define settings for all inputs in the group, or expand a device group, and select the required input.

The properties of the selected input, or the common properties for all inputs in a selected device group, will be displayed on the following tabs: *Settings*, *Info*, and *Events*.

To learn more about the properties of the selected input, or the common properties for all inputs in a selected device group, see:

Viewing the Current State of an Input

The change of an input's state is regarded as an event by RC-E. Events can be used in rules and hereby trigger actions when the state of an input is changed.

See Define Input- and Output-Related Rules (on page 94) for more information about how to include an input event in a rule.

To view the current state of an input in the Management Client, do the following:

1. In the Site Navigation pane (see "Panes Overview" on page 36), expand *Devices*, and select *Inputs*.
2. In the Overview pane (see "Panes Overview" on page 36), expand the required inputs folder and select the required input.

   Tip: You may select a group of inputs to view the current status of all inputs in the group.

3. Information about the current status of the selected input is presented in the preview pane.

   When an input is deactivated, it is shown by a gray indicator:

   When the input is activated, the indicator lights up green:

Fill in Properties on the Info Tab

Lets you view and edit basic information about an input. Contains the following fields:

- ***Name**:* Name of the input. Not compulsory, but highly recommended. Used whenever the input is listed in RC-E and clients. Does not have to be unique.

  To change the name, overwrite the existing name and click *Save* in the toolbar (see "Management Client Overview" on page 34).

  Tip: If you change the name, it will be updated throughout RC-E. This means that if the name is used in, for example, a rule, the name will automatically change in the rule as well.

- ***Description**:* Description of the input. Not compulsory. Will appear in a number of listings within RC-E. For example, the description will appear when pausing the mouse pointer over the item's name in the Overview pane (see "Panes Overview" on page 36):

To specify a description, type the description and click *Save* in the toolbar (see "Management Client Overview" on page 34).

- ***Hardware name:*** Name of the hardware with which the input unit is connected. The field is non-editable from here, but can be changed by clicking *Go To* next to it. This takes you to hardware information, where the name is editable.
- ***Unit number:*** Non-editable field, displaying the unit on which the input can be found on the hardware. For hardware capable of having more than one input unit attached, the unit number will typically indicate the number of the input port to which the input is attached. For hardware with, for example, four input ports, the numbers will typically range from *0* to *3*.

Fill in Properties on the Settings Tab

Lets you verify or edit key input settings, for a selected input, or for all inputs within a selected device group. If the selected device group contains 400 or more inputs, the *Settings* tab will be unavailable for viewing and editing because changing settings for so many devices in one step takes too long time.

The content of the *Settings* tab is determined entirely by the devices in question, and is thus likely to vary depending on the input selected.

Content may vary, but you will typically see the following property:

- ***Input rises on:*** Lets you define whether the input signal should be considered rising on *Circuit closed* or *Circuit open*. The value of this setting is used on the input's *Events* tab, where you define properties for input events: *Input Rising* event, *Input Falling* event, and *Input Changed* event. See also the description of the properties of the *Events tab* (see "*Fill in Properties on the Events Tab*" on page 90).

The content of the *Settings* tab is displayed in a table, in which the first column lists the available settings, and the second column lists the value of each setting.

You are typically able to change the values:

1. Select the row with the property you want to change
2. Click the button to the right of the properties column.
3. Change the value of the property.
4. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

When you have changed a setting to a non-default value, the value will appear in **bold**. When a value must be within a certain range, for example between 0 and 100, the allowed range will be displayed in the gray information box below the settings table.

Fill in Properties on the Events Tab

Lets you define events based on changes of the input's state, from circuit opened to circuit closed or the reverse order. The events you define can subsequently be used in rules.

You can define events for a selected input, but not for all inputs in a device group.

1. In the Site Navigation pane (see "Panes Overview" on page 36), expand *Devices*, and select *Inputs*.
2. In the Overview pane (see "Panes Overview" on page 36), select the required input.
3. Select the *Events* tab, and click *Add...*.
4. In the *Select Driver Event* dialog, select the appropriate option (*Input Rising event*, *Input Falling event*, or *Input Changed event*).

5. Click *OK*. Your selected type of input event will now appear in the *Events* tab's *Configured events* list.

To the right of the list, settings for the selected input event are displayed in a table. The table's first column lists available settings, the second column lists the value of each setting.

The settings on the *Events* tab is determined entirely by the devices in question, and is thus likely to vary depending on the input selected.

Content may vary, but you will typically see the following property:

- ***Enabled**:* Select between *True* (enabled), or *False* (disabled).

You are typically able to change the values:

1. Select the row with the property you want to change.
2. Click the button to the right of the properties column.
3. Change the value of the property.
4. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

When you have changed a setting to a non-default value, the value will appear in **bold**. When a value must be within a certain range, for example between 0 and 100, the allowed range will be displayed in the grey information box below the settings table.

Manage Output

On many devices you are able to attach external units to output ports on the device. This allows you to activate/deactivate lights, sirens, etc. through RC-E.

Output may be used when creating rules (see "Manage Rules" on page 133). You can create rules that automatically activate or deactivate outputs, and rules that trigger actions when the state of an output is changed.

Output can also be triggered manually from the Management Client and the *Ocularis Client.*

Devices' output ports are automatically detected when you add the devices to RC-E through the Management Client's *Add Hardware* (see "*Add Hardware (Cameras, etc.)*" on page 49) wizard, regardless of which of the wizard's detection options you use. By default, output are disabled. You can enable output when needed.

You have two entry points for managing outputs:

- In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Devices*, select *Outputs*, expand the required device group, and select the required output. If no device groups are available, you must first group your output: See About Device Groups (on page 95) for information about creating groups as well as adding output to your groups.
- In the Management Client's Site Navigation pane, expand *Servers* and select *Recording Servers*, then in the overview pan (see "Panes Overview" on page 36)e expand the required recording server and select the required output.

Before you specify use of external input and output units on a device, verify that sensor operation is recognized by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the RC-E release notes to verify that input- and output-controlled operations are supported for the devices and firmware used.

Enabling Output

When outputs are detected with the *Add Hardware* (see "*Add Hardware (Cameras, etc.)*" on page 49) process, they are by default disabled. You can activate outputs when needed.

If a device has several outputs you can enable one, some, or all of them as required.

1. In the Site Navigation pane (see "Panes Overview" on page 36), expand *Servers* and select *Recording Servers*.
2. In the Overview pane (see "Panes Overview" on page 36) select the relevant recording server, and find the device on which the output is placed.
3. Right-click the required output, and select *Enabled*.

Specifying Output Properties

Each output has several properties which can be found on the output's *Settings* and *Info* tabs. You can access these tabs in two ways:

- In the Site Navigation pane (see "Panes Overview" on page 36), expand *Devices* and select *Outputs*, then in the Overview pane expand the required outputs folder and select the required output.

- or -

- In the Overview pane (see "Panes Overview" on page 36), select a device group to change the settings for all outputs in this group, or expand a device group and select the required output.

The properties of the selected output, or the common properties for all outputs in a selected device group, will be displayed on the following tabs: *Settings* and *Info*.

To learn more about the properties of the selected output, or the common properties for all outputs in a selected device group, see:

Automatic and Manual Activation of Output

Output can be activated automatically or manually:

- **Automatic Activation of Output**
  With the Management Client's rules (see "Manage Rules" on page 133) feature, you are able to create rules that automatically activate or deactivate output, and rules that trigger actions when the state of an output is changed.

- For example, you may create a rule specifying that a siren should sound if motion is detected on a particular camera, or you may create a rule specifying that a camera should start recording if a siren sounds. See Define Input- and Output-Related Rules (on page 94) for more information.

- **Manual Activation of Output**
  Output may be activated manually from the Management Client and the **Ocularis Client:**

  1. In the Site Navigation pane (see "Panes Overview" on page 36), expand *Devices* and select *Outputs*.
  2. In the Overview pane (see "Panes Overview" on page 36), expand the required outputs folder and select the required output.

     Tip: You may select a group of outputs, for example *All Outputs*, to manually activate all outputs in the group.

     The availability of features for manually activating an output depends entirely on the device in question, and may thus vary.

     Typically, the following elements are shown for each output in the preview pane:

  3. Select/clear the check box to activate/deactivate the selected output. When an output is activated, the indicator lights up green:

     Alternatively, click the rectangular button to activate the output for the duration defined in the *Output Trigger Time* setting on the *Settings* tab (this feature/setting may not be available for all outputs). After the defined duration, the output is automatically deactivated.

Fill in Properties on the Info Tab

Lets you view and edit basic information about an output:

- ***Name*:** Name of the output. Not compulsory, but highly recommended. Used whenever the output is listed in RC-E and clients. Does not have to be unique.
- To change the name, overwrite the existing name and click *Save* in the toolbar (see "Management Client Overview" on page 34).

  Tip: If you change the name, it will be updated throughout RC-E. This means that if the name is used in, for example, a rule, the name will automatically change in the rule as well.
- ***Description*:** Description of the output. Not compulsory. Will appear in a number of listings within RC-E. For example, the description will appear when pausing the mouse pointer over the item's name in the Overview pane (see "Panes Overview" on page 36):

  To specify a description, type the description and click *Save* in the toolbar (see "Management Client Overview" on page 34).
- ***Hardware name*:** Name of the hardware with which the output unit is connected. The field is non-editable from here, but can be changed by clicking *Go To* next to it. This takes you to hardware information, where the name is editable.
- ***Unit number:*** Non-editable field, displaying the unit on which the output can be found on the hardware. For hardware capable of having more than one output unit attached, the unit number will typically indicate the number of the output port to which the output is attached. For hardware with, for example, four output ports, the numbers will typically range from *0* to *3*.

Fill in Properties on the Settings Tab

Lets you verify or edit key output settings, such as active output state, output trigger time, etc., for a selected output, or for all outputs within a selected device group. However, if the device group contains 400 cameras or more the *Settings* tab will not be available for viewing and editing because changing settings for so many devices in one step takes too long time.

The content of the *Settings* tab is determined entirely by the drivers for the cameras in question, and is thus likely to vary depending on the output selected.

Some devices are only able to apply outputs for a relatively short time, for example max. 5 seconds. Refer to the documentation for the device in question for exact information.

Content is displayed in a table, in which the first column lists the available settings, and the second column lists the value of each setting.

You are typically able to change the values:

1. Select the row with the property you want to change
2. Click the button to the right of the properties column.
3. Change the value of the property.
4. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

When you have changed a setting to a non-default value, the value will appear in **bold**. When a value must be within a certain range, for example between 0 and 100, the allowed range will be displayed in the grey information box below the settings table.

Define Input- and Output-Related Rules

To be able to automatically

- activate an output or trigger an event activated by an output, you must, after you have enabled an output,
- trigger an action activated by an input, you must, after you have enabled the input and created an event based on the input, include it in a rule.

See Manage Output (on page 91) or Manage Input (on page 88) for more information.

For example, you may create a rule specifying that:

- a siren should sound if motion is detected on a particular camera, or you may create a rule specifying that a camera should start recording if a siren sounds (output).
- a camera should record if a particular input is activated (input).

For the following examples to be useful you should have general knowledge about managing rules (see "Manage Rules" on page 133). See also Create Typical Rules (on page 116) for other step-by-step descriptions of how to create rules.

Tip: When you create a rule based on an in- or output event, the actions you specify in the rule do not have to relate to the device on which the external in- or output was activated; you can easily specify that the actions should take place on one or more different devices— even across recording servers.

Defining a Rule that Activates/Deactivates an Output

1. Start the *Manage Rule* and in step 1 select a rule type and, if necessary, a condition in step 2.
2. In *Manage Rule*'s step 3 (*Step 3: Actions*) select the *Set device output to* <*state*> action.
3. If you like the output to be activated/deactivated immediately, skip this step. If you do not want to activate or deactivate the output immediately after the event, click the *immediately* link in the initial rule description, and select an interval between the event and the activation/deactivation of the output. Click *OK* to confirm your selection.
4. Click the *state* link in the initial rule description, and select whether you want to activate or deactivate the output. Click *OK* to confirm your selection.
5. Click the *devices* link in the initial rule description, and select which output you want to activate or deactivate. Click *OK* to confirm your selection.
6. If wanted you can select more actions in the *Manage Rule*'s step 3 (*Step 3: Actions*). Do so or simply click *Next* to continue to the next step.
7. In *Manage Rule*'s step 4 (*Step 4: Stop criteria*) select one of the stop actions, for instance to deactivate the output after a certain time or event.
8. Click *Finish* to save the rule.

Defining a Rule where an Output Triggers an Action

In the *Rules* feature, all registered external output (activation, deactivation or change) is treated as an event. Based on an event, you are able to specify a wide variety of actions to take.

To define a rule where an output activates an action, do the following:

1. Start the *Manage Rule*.
2. In *Manage Rule*'s step 1 (*Step 1: Type of rule*) select the *Perform an action on* <*event* > option.

3. Click the *event* link in the initial rule description.
4. In the *Select an Event* dialog's *Built-in* group, select the appropriate option for your rule: *Output Activated*, *Output Changed* or *Output Deactivated*. Click *OK* to confirm your selection.
5. Click the *devices/recorders/servers* link in the initial rule description.
6. In the *Select Devices and Groups* dialog select the required output. Click *OK* to confirm your selection.
7. Click *Next* to continue to the *Manage Rule*'s step 2 (*Step 2: Conditions*) and select, if necessary, a condition.
8. Continue to step 3 (*Step 3:Actions*) and select one or more actions.
9. If you do not want to define a stop action, skip this step. If you want to define a stop action— for instance to deactivate the output again— click *Next* to continue to step 4 (*Step 4: Stop criteria*), and select a stop action.
10. Click *Finish* to save the rule.

Defining a Rule where an Input Triggers an Action

In the *Rules* feature, all registered external input (activation, deactivation, or change) is treated as an event. Based on an event, you are able to specify a wide variety of actions to take.

To define a rule specifying that an input should result in one or more actions (for example the starting of recording on a certain camera), do the following:

1. Start *Managing Rules*.
2. In *Managing Rules* step 1 (*Step 1: Type of rule*) select the *Perform an action on <event >* option.
3. Click the *event* link in the initial rule description.
4. In the *Select an Event* dialog's *Hardware Configurable* group, select the appropriate option for your rule: *Input Activated*, *Input Changed*, or *Input Deactivated*. Click *OK* to confirm your selection.
5. Click the *devices/recording servers/management servers* link in the initial rule description.
6. In the *Select Devices and Groups* dialog select the required input. Click *OK* to confirm your selection.
7. Click *Next* to continue to *Managing Rules* step 2 (*Step 2: Conditions*) and select, if necessary, a condition.
8. Continue to step 3 (*Step 3:Actions*) and select one or more actions.
9. Click *Next* to continue to step 4 (*Step 4: Stop criteria*), and select a stop criteria. **Click** *Next* **to continue to step 5 (Step 5: Stop actions), and select a stop action.**
10. Click *Finish* to save the rule.

About Device Groups

You are able to group different types of devices (cameras, microphones, speakers, inputs, outputs) on your RC-E system by using device groups. The use of device groups has several benefits:

- Device groups help you maintain an intuitive overview of devices on your system
- You are able to specify common properties for all devices within a device group in one step
- When dealing with roles (see "About Roles" on page 145), you are able to specify common security settings for all devices within a device group in one step

- When dealing with rules (see "Manage Rules" on page 133), you are able to apply a rule for all devices within a device group in one step

You can add as many device groups as required; you are completely free to decide which devices to include. The only restriction is that you cannot mix different types of devices (for example cameras and speakers) in a device group.

If a device group contains 400 devices or more, the *Settings* tab is unavailable for viewing and editing. For camera groups, the *Streams* tab is also unavailable for editing and viewing if the group contains 400 cameras or more. When you click the plus sign next to the device folder, your RC-E system will load the contents of the device folder, which may take a few seconds. While expanding, the text *(expanding...)* is displayed next to the folder name.

The following examples are based on grouping cameras into device groups, but the principle applies for microphones, speakers, inputs and outputs as well.

Adding a Device Group

1. In the overview pane (see "Panes Overview" on page 36), right-click the item under which you wish to create the new device group.
2. Select *Add Device Group*:

   Tip: You may also simply press CTRL+N on your keyboard.

   The *Add Device Group* dialog will appear.
3. In the *Add Device Group* dialog, specify a name and description of the new device group:

   The description will later appear when pausing the mouse pointer over the device group in the device list.
4. Click *OK*. A folder representing the new device group is added to the list. You are now able to specify which devices should belong in the device group.

   Tip: If required, you are able to add device groups as subgroups under other device groups, as illustrated here:

Specifying Which Devices to Include in a Device Group

1. In the Overview pane (see "Panes Overview" on page 36)'s device list, right-click the required device group folder.
2. Select *Edit Device Group Members.* The *Select Group Members* window will appear.
3. In the *Select Group Members* window, select either:
   - The *Device Groups* tab, which lists devices based on existing device groups.

     Tip: A device can be a member of more than one device group.
   - The *Recording Servers* tab, which lists devices based on which recording servers the devices belong on.
4. Select the devices you wish to include, and click *Add* . This will copy the selected devices to the *Selected* box:

   Tip: You may also double-click a device to copy it from one box to the other, or you may simply drag devices between the two boxes.

   Tip: To select several devices in one step, press the CTRL key on your keyboard while selecting.
5. Click *OK*. The selected devices will be added to your device group on the device list.

Specifying Common Settings for All Devices in a Device Group

When using device groups, you are able to quickly specify common properties for all devices within a given device group:

1. In the overview pane (see "Panes Overview" on page 36)'s device list, click the required device group.

   In the properties pane (see "Panes Overview" on page 36), all properties *which are available on all of the device group's devices* will be listed, grouped on tabs.

2. Specify the required common properties.

   Properties not available on *all* of the devices in the device group will not be listed; such properties must still be configured individually for each device.

   If the device group contains 400 or more devices the *Settings* tab is unavailable for viewing and editing. For camera groups the *Streams* tab is also unavailable for viewing and editing if the group contains 400 cameras or more.

   Tip: The Settings tab (see "Enabling and Disabling Edge Recording—Camera Only" on page 106) has convenient functionality for quickly switching between settings for the device group and settings for individual devices.

Deleting a Device Group

1. In the overview pane (see "Panes Overview" on page 36)'s device list, right-click the unwanted device group folder.
2. Select *Delete Group*.

   Tip: You may also simply press DELETE on your keyboard.

3. You will be asked to confirm that you want to delete the device group. Verify that you are deleting the correct device group, then click *Yes*.

Remember that you have only deleted the device group itself. If you wish to delete IP hardware - such as a camera - from your RC-E system, do so on a recording server level (see Managing Hardware (see "Manage Hardware" on page 53)).

About Events

Events are primarily used for triggering actions. Actions are configurable through rules **(see "**Manage Rules**" on page 133).**

Example: You create a rule which specifies that in the *event* of detected motion, the surveillance system should take the *action* of starting recording of video from a particular camera.

In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), you are able to work with the following under *Rules and Events*:

- ***Rules*** (see "Manage Rules" on page 133)***:*** Rules are a central element in RC-E. The behavior of your surveillance system is to a very large extent determined by rules.
- ***Time profiles*** (see "Manage Time Profiles" on page 138)***:*** Time profiles are periods of time defined in the Management Client. They can be used when creating rules in the Management Client; for example, to create a rule which specifies that a certain action should take place within a certain time profile.

- ***Notification Profiles*** (see "Manage Notification Profiles" on page 141)***:*** With notification profiles you can set up ready-made e-mail notifications, which can automatically be triggered by a rule, for example when a particular event occurs.

- ***User-defined Events*** (see "Manage User-defined Events" on page 143)***:*** User-defined events are custom made events making it possible for users to manually trigger events in the system or react to inputs from the system.

- ***Hardware Configurable Events:*** (see "Hardware Configurable Events" on page 110)Some hardware is capable of creating events themselves. For example, some cameras are themselves able to detect motion or static/moving objects, and their detections can be used as events in RC-E. Such events must obviously be configured on the hardware before they can be used in RC-E , therefore they are called hardware configurable events. Read more about hardware configurable events for cameras (see "Manage Cameras" on page 75), inputs (see "Manage Input" on page 88) and microphones (see "Manage Microphones" on page 85) respectively.

See Events Overview (on page 128) for a list of events.

About Multi-streaming

Viewing of live video and playing back of recorded video does not necessarily require the same settings to achieve the best result. To handle this, RC-E and some cameras support multi-streaming, with which you can establish two independent streams to the recording server. **Either** one stream for live viewing and another stream for playback purposes **or** two separate live streams—with different resolution, encoding, and frame rate.

Example 1, live and recorded video:

- For viewing **live** video, your organization may prefer MPEG4 at a high frame rate.

- For playing back **recorded** video, your organization may prefer MJPEG at a lower frame rate because this will help preserve disk space.

Example 2, two live videos:

- For viewing **live video from a local operating point**, your organization may prefer MPEG4 at a high frame rate to have the highest quality of video available.

- For viewing **live video from a remotely connected operating point**, your organization may prefer MJPEG at a lower frame rate and quality in order to preserve network bandwidth.

Even when cameras support multi-streaming, individual multi-streaming capabilities may vary considerably between different cameras. Refer to camera's documentation for exact information. To see if a camera offers different types of streams, see the *Settings* tab (see "Settings Tab Overview" on page 106).

You manage multi-streaming on the *Streams* tab. The tab is only available when the selected camera or device group supports multi-streaming.

If you select a device group with 400 or more cameras, the *Streams* tab will not be available for viewing and editing because changing settings for so many devices in one step takes too long time.

To access the *Streams* tab, expand *Devices* in the Management Client's Site navigation pane (see "Panes Overview" on page 36), expand the relevant camera folder in the Overview pane (see "Panes Overview" on page 36), select the required camera and then select the *Streams* tab in the Properties pane (see "Panes Overview" on page 36).

The tab will by default list a single stream—the selected camera's default stream, used for live video as well as for video which is being recorded for playback purposes.

Note that while it is possible to set up and use two live streams, only one of the enabled live streams is able to record video at a time. To change which stream to use for recording, use the *Record* box.

Adding a New Stream

1. On the *Streams* tab, click *Add*. This will add a second stream to the list (you cannot have more than two streams).
2. In the *Stream* column, select the required type of stream.
3. If you want to use the stream for live video, select the check box in the *Live* column. Leave the check box cleared if you only want to use the stream for video which will be recorded.

   You can use the same stream for both live and recorded video if required. You cannot use two different streams for the same purpose, for example for live video.
4. If you want to use the stream for recorded video, select the check box in the *Record* column. Leave the check box cleared if you only want to use the stream for live video.

   Note how the selection in the *Plug-ins* column always follows the stream you have selected for recorded video. This is because the integrated plug-in which RC-E uses for motion detection is always applied on the video stream which will be recorded.

   The *Edge Recording* column indicates whether the selected stream supports edge recording (see "Record Tab Overview" on page 103) or not.
5. Click *Save.*

Events Tab Overview

For items (cameras or microphones) supporting events, you are able to manage the hardware configurable events on the *Events* tab. To access the *Events* tab, select the required item in the overview pane (see "Panes Overview" on page 36), then select the *Events* tab in the properties pane (see "Panes Overview" on page 36).

The *Events* tab will only be available if the selected item supports hardware configurable events.

Even when an item supports hardware configurable events, it is always your decision whether you want to use such events on your RC-E system. Therefore, you simply add each hardware configurable event you want to be able to use on each item.

About the Event Tab for Camera

In addition to RC-E's motion detection, some cameras can themselves be configured to detect motion. If a camera is capable of such detection, the camera's detections can be used as events. Such events can in turn be used when creating event-based rules (see "Events Overview" on page 128). Events from cameras are called hardware configurable events as they technically occur on the actual camera hardware rather than on the surveillance system.

Even though events based on signals from input and/or output units connected to camera devices are technically also hardware configurable events, they are managed elsewhere. See Manage Inputs (see "Manage Input" on page 88) and Manage Outputs (see "Manage Output" on page 91).

About the Event Tab for Microphone

Some devices are capable of creating events themselves. Such events can in be used when creating event-based rules (see "Events Overview" on page 128) in RC-E. Events from such devices are called hardware configurable events, as they technically occur on the actual camera hardware rather than on the surveillance system.

Adding a Hardware Configurable Event

1. On the *Events* Tab, click *Add...*. This opens the *Select Driver Event* window.

2. Select the required hardware configurable event:

   You can only select one hardware configurable event at a time.

3. Click *OK*. The selected event will be added to the *Events* tab's list of configured events.

4. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

Using Several Instances of a Hardware Configurable Event

To be able to specify different properties for different instances of an event, you are able to add a hardware configurable event more than once (see also Specifying Hardware Configurable Event Properties (see "Specify Hardware Configurable Event Properties" on page 100)).

The following example is specific to **cameras**.

Example: The camera in question has been configured with two motion windows, called A1, and A2. You have added two instances of the *Motion Started (HW)* event. In the properties of one instance, you have specified use of motion window A1; in the properties of the other instance, you have specified use of motion window A2.

When you use the hardware configurable event in a rule, you are able to specify that the event should be based on motion detected in a specific motion window in order for the rule to be triggered:

Deleting a Hardware Configurable Event

Bear in mind that deleting a hardware configurable event will affect any rules in which the event is used.

1. In the *Events* tab's *Configured Events* list, select the no longer required event.

   Tip: If there are several instances of the same event, use the properties list in the right side of the tab to verify that you have selected the correct event.

2. Click *Delete*.

   The selected event will be deleted without further warning.

3. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

Specify Hardware Configurable Event Properties

For each hardware configurable event you have added, you are able to specify properties. The number of properties depends on the item in question. In order to work as intended, some or all of the properties must be specified identically on the item as well as on RC-E.

Even though the following list is not exhaustive, you may often be able to specify the following properties:

- ***Enabled***: Determines whether use of the hardware configurable event is enabled. Select *True* to enable; select *False* to disable.

  Enabled is the only property you will always see for microphones.

- ***Include Images:*** Determines whether video should be sent from the camera to RC-E when the event occurs. Select *True* if video is required; select *False* if video is not required.

- ***Motion Window:*** Many cameras capable of detecting motion can be configured with different motion detection settings for different parts the camera's images. For example, if a camera covers a 2-lane road, different motion detection settings may have been defined for the right lane and left lane area of the camera's images. Such areas are generally known as motion windows.

Provided one or more motion windows have been defined on the camera device, the *Motion Window* setting lets you specify which motion window to use for the event. When the camera detects motion within the specified motion window, the event will occur.

When specifying use of a motion window, make sure you type the name of the motion window, exactly as it has been specified on the camera.

You can only specify one motion window in the field. However, you are able to add more than one instance of an event (see "Using Several Instances of a Hardware Configurable Event" on page 100).

- ***Prebuffer frames per second*** **:** Determines the frame rate to be used for prebuffered video. See also the next description of *Prebuffered Seconds* setting.
- ***Prebuffer Seconds*** **:** Determines the number of seconds for which video from the camera should be stored for possible later use.

  What does "prebuffer" mean? Prebuffering is essentially the ability to store video from before the initial boundaries of a recording. It allows you to view video from *before* an event occurred.

If, for example, you are going to use the hardware configurable event in an rule specifying that recording should start when the event occurs, being able to see what happened immediately prior to the door being opened may also be important.

Example: If using five seconds of prebuffering, video from the camera will always be stored provisionally for five seconds. If the event occurs, five seconds' worth of video will be available for attaching to any recording triggered by the event, as specified in a rule.

Info Tab Overview

The *Info* tab lets you view and edit basic information about a selected item in a number of fields. The following items under *Devices* have an *Info* tab:

- Cameras (see "Manage Cameras" on page 75)
- Hardware (see "Manage Hardware" on page 53)
- Microphones (see "Manage Microphones" on page 85)
- Speakers (see "Manage Speakers" on page 87)

Description of Info Tab's Fields

- ***Name***: Name of the item. Not compulsory, but highly recommended. Used whenever the item is listed in RC-E and clients. Does not have to be unique.

  To change the name, overwrite the existing name and click *Save* in the toolbar (see "Management Client Overview" on page 34).

  Tip: If you change the name, it will be updated throughout RC-E. This means that if the name is used in, for example, a rule, the name will automatically change in the rule as well.

- ***Description***: Description of the item. Not compulsory. Will appear in a number of listings within RC-E. For example, the description will appear when pausing the mouse pointer over the item's name in the overview pane:

  To specify a description, type the description and click *Save* in the toolbar (see "Management Client Overview" on page 34).

- ***Hardware name***: (only relevant for Camera, Microphone and Speaker) Name of the hardware, with which the item is connected. The field is non-editable from here, but can be changed by clicking *Go To* next to it. This will take you to hardware information, where the name is editable.
- ***Unit number***: (only relevant for Camera, Microphone and Speaker) Non-editable field displaying the unit on which the item is attached on the hardware.

  For single-device hardware, the unit number will typically be *1*. For multi-device hardware, such as video servers with several channels, the unit number will typically indicate the channel on which the item is attached, e.g. *3*.
- ***Shortcut***: (only relevant for Camera) Users of the Ocularis Client can take advantage of a range of keyboard shortcuts, some of which let the user toggle between viewing different cameras. Such shortcuts include numbers used to identify each camera. In the Management Client, each camera's shortcut number is specified in the *Shortcut* field.

  A camera shortcut number cannot contain letters or special characters, and must be no longer than four digits:

  - Examples of correct camera shortcut numbers: *3*, *1234*.
  - Examples of incorrect camera shortcut numbers: *A*3*, *12345*.

  It is highly recommended that you use a unique camera shortcut number for each camera.

  Tip: Find more information about keyboard shortcuts from a Ocularis Client user's perspective in the separate Ocularis Client documentation available on the OnSSI RC-E software DVD as well as from www.onssi.com (http://www.onssi.com)
- ***Serial Number:*** (only relevant for Hardware) Hardware serial number as specified by the manufacturer. The serial number is often, but not always, identical to the MAC address.
- ***Firmware version:*** (only relevant for Hardware) Firmware version as specified by the manufacturer.
- ***MAC address:*** (only relevant for Hardware) Hardware MAC address. A MAC (Media Access Control) address is a 12-character hexadecimal number uniquely identifying each device on a network.
- ***Product ID***: (only relevant for Hardware) Product identifier.
- ***Hardware host name:*** (only relevant for Hardware) Host name or IP address of the hardware.

Tip: By clicking the button next to the field, you are able to connect to the hardware's own configuration page. The page opens in a separate window.

PTZ Tab (Hardware Properties)

The *PTZ* tab lets your enable PTZ (Pan/Tilt/Zoom) for video encoders. It is only available if the selected hardware is a video encoder.

What is a video encoder? A video encoder, also known as video server, is a piece of hardware which is able to stream video from a number of connected cameras. Video encoders contain image digitizers, making it possible to connect analog cameras to a network.

For video encoders, the use of PTZ must be enabled on the hardware level before you can use the PTZ features of PTZ cameras attached to the video encoder. The *Settings* tab lets you enable the use of PTZ separately for each of the video encoder's channels.

To access the *PTZ* tab, select the required hardware in the overview pane (see "Panes Overview" on page 36), then select the *PTZ* tab in the properties pane (see "Panes Overview" on page 36).

Not all video encoders support the use of PTZ cameras. Even video encoders which support the use of PTZ cameras may require configuration, such as installation of additional drivers (typically through accessing a browser-based configuration interface on the device's IP address) before PTZ cameras can be used.

Enabling PTZ on a Video Encoder

To enable the use of PTZ cameras on a video encoder, do the following on the *PTZ* tab:

1. In the list of devices connected to the video encoder, select the *Enable PTZ* box for the camera(s) on which you want to use PTZ:
2. In the *PTZ Device ID* column, verify the ID of the PTZ camera(s) in question.
3. In the *COM Port* column, select which of the video encoder's COM (serial communications) ports should be used for controlling PTZ functionality on each required PTZ camera:
4. In the *PTZ Protocol* column, select which positioning scheme to use for each required PTZ camera:
   - ***Absolute*:** When operators use Pan/Tilt/Zoom controls for the camera, the camera is adjusted relative to a fixed position, often referred to as the camera's home position
   - ***Relative*:** When operators use Pan/Tilt/Zoom controls for the camera, the camera is adjusted relative to its current position

   Refer to the camera's documentation if in doubt.
5. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

   You are now able to configure preset positions (see "PTZ Presets Tab (Camera Properties)" on page 83) and patrolling (see "PTZ Patrolling Tab (Camera Properties)" on page 80) for the PTZ camera(s) in question.

Record Tab Overview

Recordings from an item (camera, microphone or speaker) will only be saved in the item's database when recording is enabled and recording-related rule (see "Manage Rules" on page 133) criteria are met.

Camera

Lets you specify recording and storage settings for the selected camera.

What does recording mean? In IP video surveillance systems, the term *recording* means *saving video from a camera in the camera's database on the surveillance system*. In many IP video surveillance systems, all of the video received from cameras is not necessarily saved. Instead, saving of video in a camera's database, i.e. recording, is started only when there is a reason to do so: For example when motion is detected, when an event occurs, or when a specific period of time begins. Recording is then stopped after a specified amount of time, when motion is no longer detected, when an event occurs, when a time period ends, or similar. The term *recording* originates from the analog video era, when video was taped only when the record button was pressed.

Microphone

Lets you specify recording and storage settings for the selected microphone. Microphones' recording and storage settings are completely independent of cameras and speakers.

Speaker

Lets you specify recording and storage settings for the selected speaker.

Enabling and Disabling Recording

Recording is by default enabled.

To enable/disable recording for the selected item, select/clear the *Record* tab's *Recording* check box.

Recording must be enabled for the item before you are able to record (i.e. save) video or audio from the camera. A rule (see "Manage Rules" on page 133) specifying that an item should record under particular circumstances will not work if recording is disabled for the item in question.

Setting Recording Frame Rate—Camera Only

Specifying recording frame rate is only possible for MJPEG, a video codec (technology for compressing and decompressing data) with which each frame is separately compressed into a JPEG image.

1. Select or type the required recording frame rate (in FPS, Frames Per Second) in the *Recording frame rate* box.

2. Clicking the *Recording frame rate* box' up/down arrows will increase/reduce the value in increments of 1 FPS.

Tip: If you click inside the *Recording frame rate* box, two decimals will be added to the value. By selecting the number before or after the separator, you are able to increase/reduce the numbers in increments of 1 unit. This way you are able to specify a very specific recording frame rate average over time, for example of 20.15 FPS:

Working with Prebuffering

Prebuffering is essentially the ability to save video and audio in the camera's or microphone's database before the initial boundaries of a recording.

Use of prebuffering can be highly advantageous: It allows you to save video and audio from **before** the events or times used to start recordings.

How Prebuffering Works for Cameras and Microphones...

If, for example, you have created a rule specifying that recording should start when a door is opened, being able to see what happened immediately prior to the door being opened may be useful. Such prebuffering is possible since RC-E continuously receives streams of video and audio from connected cameras and microphones (unless the transfer of video or audio from cameras or microphones has in some way been disabled). Storing video and audio from before the initial boundaries of a recording is therefore not a problem: video and audio passes through RC-E anyway.

When prebuffering is enabled for a camera or a microphone, RC-E continuously records video or audio from the camera's or microphones stream and provisionally stores it in the database for a specified number of seconds before automatically deleting it— unless the provisionally stored video or audio turns out to be required for a recording, in which case it is automatically added to the recording.

How Prebuffering Works for Speakers...

Unlike video and incoming audio, which RC-E continuously receives from connected cameras and microphones, outgoing audio is only transmitted when Ocularis Client users press a button to talk through speakers. This can, depending on which events or times are used to start recordings, mean that there will be very little or no outgoing audio available for prebuffering.

Enabling and Disabling Prebuffering

Prebuffering is by default enabled; with a prebuffer size of 3 seconds. To enable/disable prebuffering, select/clear the *Enable prebuffering* check box. When enabling, remember to specify a prebuffer size.

Specifying Prebuffer

Select or type the required prebuffer size (in seconds) in the *Prebuffer size* box. Clicking the *Prebuffer size* box' up/down arrows will increase/reduce the value in increments of one second.

The number of seconds you specify in the *Prebuffer size* box must be sufficiently large to accommodate your requirements.

> **Example:** If, like in this rule example, you plan to be able to save video from five seconds prior to detected motion, the prebuffer size must be at least five seconds.

Using Prebuffering in Rules

The use of prebuffering enables you to create rules (see "Manage Rules" on page 133) specifying that recording should begin prior to the event or time triggering the rule.

> **Example:** Your ability to use this example rule— specifying that recording should start on a camera 5 seconds before motion is detected on the camera— depends on prebuffering being enabled for the camera in question.

Working with Storage Area

In the *Storage* area you can monitor and edit database settings for the selected item.

At the top of the *Storage* area, the selected database for the item in question and its status is stated. In this example, the selected database is *Local Default* and its status is *Active*.

Possible Statuses for Selected Database:

- ***Active*** *- database is active and running.*
- ***Archives also located in old storage*** - database is active and running and has archives located in other storage areas as well.
- ***Data for some of the devices chosen is currently moving to another location*** - database is active and running and moving data from one or more selected devices from one location to another.
- ***Data for the device is currently moving to another location*** - database is active and running and moving data from the selected device is currently moving from one location to another.
- ***Information unavailable in failover mode -***status information about the database cannot be collected when database is in failover mode. See Manage Failover Servers (on page 192).

Further down in the *Storage* area it is also possible to see which archive(s) are associated with the selected database, their individual status (***OK*** or ***Old Storage***), location and how much space they each use.

In the *Total used space* field, the total spaced used for the entire storage is indicated.

Selecting a Different Storage:

1. In the upper part of the *Storage* area, click *Select...* to change database for the item in question.
2. In the *Select Storage* dialog that follows, select the wanted database.
3. Click *OK*.
4. Next, in the *Recordings Action* dialog, select whether already existing—**non-archived**—recordings should be moved along to the new storage or deleted.
5. After selecting, click *OK*.

Deleting All Recordings:

1. To delete all recordings for the selected item, click *Delete All Recordings* at the bottom of the *Storage* area.
2. Click *Yes*.

Enabling and Disabling Edge Recording—Camera Only

The *Edge recording* area will only be enabled if the selected camera supports edge recording.

If disabled, select the *Use edge recording if device is unavailable* check box to enable edge recording.

Note that the *Retrieve edge storage recordings from <devices>* rule (see "Actions and Stop Actions Overview" on page 110) can be used independently of this setting.

IMPORTANT: Edge recording cannot coexist with pre-alarm image functionality (see "Actions and Stop Actions Overview" on page 110), action *Send notification to <profile>*). So if a camera is setup to do edge recording, it is not possible to export pre-alarm images from that camera, and vice versa.

What is edge recording? Some cameras are capable of edge recording. This means, that to minimize loss in case connection between the camera and the recording server is lost or broken unexpectedly, they are able to use their own local storage to store recorded video and audio. In that case, cameras with edge recording capabilities can record on their own storage and when communication is re-established, recordings are transferred from the camera to the surveillance system.

Your organization may not want to retrieve recordings from a camera at all times, but rather retrieve it from the camera's edge storage at a specific time of day to save bandwidth, for example, if your organization has cameras in several locations and a Recording Server situated at a central location away from the cameras. To avoid constantly having traffic on the network connection between the cameras and the recording server, your organization can then set up a rule (see "Manage Rules" on page 133) which on a specific time, or within a Time Profile (see "Manage Time Profiles" on page 138), retrieves recordings within a specified time interval, for example eight hours of recordings during business hours which are transferring from the cameras' edge storages to the Recording Server during your organization's closing hours.

Settings Tab Overview

If you select a device group with 400 or more items the *Settings* tab will not be available for editing because changing settings for so many devices in one step takes too long time.

The content of the *Settings* tab is displayed in a table, in which the first column lists the available settings, and the second column lists the value of each setting. You are typically able to change values; when you have changed a setting to a non-default value, the value will appear **in bold**. When a value must be within a certain range, for example between 0 and 100, the allowed range will be displayed in the information box below the settings table:

1. In the Management Client's overview pane (see "Panes Overview" on page 36), right-click the required recording server to see its device groups. Select the relevant hardware under the wanted device group. On the *Settings* tab, all settings which are common to all of the device group's hardware will be listed.
2. Select if you want to enable HTTPS on the hardware device. This is not enabled by default.
3. Enter the port to which the HTTPS connection is connected. The port number can be any numeric value between 1 and 65535.
4. Make changes as needed
5. Click *Save*.

HTTPS is enabled for the entire hardware device, that is, for example, a hardware device’s camera, microphone and speaker.

Camera

Lets you verify or edit settings, such as default frame rate, resolution, compression, the maximum number of frames between keyframes, on-screen date/time/text display, etc., for a selected camera, or for all cameras within a selected device group.

The content of the *Settings* tab is determined entirely by the drivers for the cameras in question, and is thus likely to vary depending on the types of cameras selected.

Tip: Some cameras may support more than one type of stream, for example MPEG4 and MJPEG. In that case, you can use multi-streaming (see "About Multi-streaming" on page 98).

Tip: If you change a camera's settings, you can quickly verify the effect of your change if you have the preview pane (see "Panes Overview" on page 36) enabled. Note, however, that you cannot use the preview pane to judge the effect of frame rate changes, as a special frame rate for the preview pane's thumbnail images is used (defined in the Options dialog (see "Options" on page 168)).

Microphone and Speaker

Lets you verify or edit settings for selected microphones and speakers, or for all microphones or speakers within a selected device group.

Content of the *Settings* tab may vary depending on the types of microphones or speakers selected.

Hardware

Lets you verify or edit settings for the hardware selected under a recording server.

The content of the *Settings* tab is determined entirely by the hardware in question, and may thus vary depending on the type of hardware selected. For some types of hardware, the *Settings* tab may display no content at all.

Specify Common Settings for All Items in a Device Group—Cameras, Microphones and Speakers

If using Device Groups (see "About Device Groups" on page 95), you are able to quickly specify common settings for all devices within a given device group:

1. In the list of device in the Management Client's Overview pane (see "Panes Overview" on page 36), right-click the required device group. On the *Settings* tab, all settings which are common to all of the device group's items (i.e. cameras, microphones or speakers) will be listed.
2. You are now able to verify or change both common settings and settings for individual item types within the device group.

   From the menu above the settings list, select the required type of item:
3. Make changes as needed.
4. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

Specify Common Settings for All Items in a Device Group—Hardware

1. In the Management Client's Overview pane (see "Panes Overview" on page 36), right-click the required recording server to see its device groups. Select the relevant hardware under the wanted device group. On the *Settings* tab, all settings which are common to all of the device group's hardware will be listed.
2. You are now able to verify or change both common settings and settings for the individual hardware types within the device group.

   From the menu above the settings list, select the required type of hardware.
3. Make changes as needed
4. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

Set Up a Secure Connection on All Items in a Device Group

1. In the Management Client's overview pane (see "Panes Overview" on page 36), right-click the required recording server to see its device groups. Select the relevant hardware under the wanted device group. On the *Settings* tab, all settings which are common to all of the device group's hardware will be listed.
2. Select if you want to enable HTTPS on the hardware device. This is not enabled by default.
3. Enter the port to which the HTTPS connection is connected. The port number can be any numeric value between 1 and 65535.
4. Make changes as needed
5. Click *Save*.

HTTPS is enabled for the entire hardware device, that is, for example, a hardware device's camera, microphone and speaker.

Client

About Clients

In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), you are able to configure various parameters for client use.

Manage View Groups

The way in which video from one or more cameras is presented in a client is called a view. A view group is basically a container for one or more logical groups of such views.

In the clients a view group is presented as an expandable folder from which users can select the group, and subsequently the view they want to see:

More about View Groups

By default, each role you define in the Management Client is also created as a view group: when you add a role in RC-E Manager, the role will by default appear as a view group for use in Ocularis Client Limited Mode.

- A view group based on a role will by default only be available to users/groups who have been assigned to the role in question. You are able to change this; see *View Group Rights* in Specify Rights of a Role (on page 150).
- A view group based on a role will by default carry the role's name.

  Example: If you create a role with the name *Building A Security Staff*, it will by default appear in Ocularis Client Limited Mode as a view group called *Building A Security Staff*. You are able to change the name; see the following for more information.
- In addition to the view groups that are created when roles are added, you are able to create as many other view groups as you require. You can also delete view groups which you do not want to use, including those automatically created when adding roles.
- Even though a view group is created each time you add a role (see "Manage Roles" on page 147), view groups do not have to correspond to roles. You are therefore able to add any number of view groups—if required—and

rename or remove each of your view groups if required. This is no matter whether the view groups were created automatically when adding a role or whether you added them manually.

Adding a View Group

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand the *Clients* node, right-click *View Groups,* and select *Add View Group.* This opens the *Add View Group* dialog.
2. Type the name of the new view group, then click *OK*.
3. Optionally; in the Management Client's Overview pane, select the added view group, then in the Properties pane add a description of the view group.

No roles will have the right to use the newly added view group until you have specified such rights; see *View Group Rights* in Specify Rights of a Role (on page 150) for more information.

Also, even when you have specified which roles should be able to use the newly added view group, already connected client users with the relevant roles must log out and log in again before they will be able to see the view group.

Renaming a View Group

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Clients* and select *View Groups.*
2. In the Management Client's Overview pane, right-click the required view group and select *Rename View Group.*
3. Change the view group's name as required, then press the return key on your keyboard.

Client users already connected must log out and log in again before the name change will be visible.

Removing a View Group

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Clients* and select *View Groups.*
2. In the Management Client's Overview pane, right-click the required view group and select *Delete View Group.*
3. Click *Yes*.

Rules and Events

About Rules and Events

Events are primarily used for triggering actions. Actions are configurable through rules **(see "**Manage Rules**" on page 133).**

> **Example:** You create a rule which specifies that in the *event* of detected motion, the surveillance system should take the *action* of starting recording of video from a particular camera.

In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), you are able to work with the following under *Rules and Events*:

- ***Rules (see "Manage Rules" on page 133): Rules are a central element in RC-E. The behavior of your surveillance system is to a very large extent determined by rules.***
- ***Time profiles*** (see "Manage Time Profiles" on page 138)***:*** Time profiles are periods of time defined in the Management Client. They can be used when creating rules in the Management Client; for example, to create a rule which specifies that a certain action should take place within a certain time profile.
- ***Notification Profiles*** (see "Manage Notification Profiles" on page 141)***:*** With notification profiles you can set up ready-made e-mail notifications, which can automatically be triggered by a rule, for example when a particular event occurs.
- ***User-defined Events*** (see "Manage User-defined Events" on page 143)***:*** User-defined events are custom made events making it possible for users to manually trigger events in the system or react to inputs from the system.
- ***Hardware Configurable Events:*** (see "Hardware Configurable Events" on page 110)Some hardware is capable of creating events themselves. For example, some cameras are themselves able to detect motion or static/moving objects, and their detections can be used as events in RC-E. Such events must obviously be configured on the hardware before they can be used in RC-E , therefore they are called hardware configurable events. Read more about hardware configurable events for cameras (see "Manage Cameras" on page 75), inputs (see "Manage Input" on page 88) and microphones (see "Manage Microphones" on page 85) respectively.

See Events Overview (on page 128) for a list of events.

User-defined Events

If the event you require is not on the *Events Overview* list, you can create your own user-defined events (see "Manage User-defined Events" on page 143). Such user-defined events can be useful if you want to integrate other systems with your surveillance system.

> **Example**: With user-defined events, you can use data received from a third-party access control system as events in RC-E; the events can subsequently trigger actions. This way, you can, for example, begin recording video from relevant cameras when somebody enters a building.

User-defined events can also be used for manually triggering events while viewing live video in the Ocularis Client.

Hardware Configurable Events

Some hardware is capable of creating events themselves. For example, some cameras are themselves able to detect motion or static/moving objects, and their detections can be used as events in RC-E. Such events must obviously be configured on the hardware before they can be used in RC-E , therefore they are called hardware configurable events. Read more about hardware configurable events for cameras (see "Manage Cameras" on page 75), inputs (see "Manage Input" on page 88) and microphones (see "Manage Microphones" on page 85) respectively.

Actions and Stop Actions Overview

When creating rules in the *Manage Rule* wizard (see Manage Rules (on page 133)), you are able to select between a number of different actions:

Some of these actions will require a subsequent stop action.

> ***Example:*** If you select the action *Start recording*, recording will start and potentially continue indefinitely. Therefore, the action *Start recording* has a compulsory stop action called *Stop recording*.

Manage Rule makes sure you specify such stop actions when necessary; stop actions are typically specified on one of the last steps of the wizard:

Each type of action is described (additional actions may, however, be available if your RC-E installation uses add-on products, special plug-ins, etc.). For each type of action, stop action information is listed as well:

Action	Description
Start recording	Begin recording, i.e. begin saving video in the database of the selected camera. When selecting this type of action, *Manage Rule* will prompt you to specify when recording should start (either immediately or a number of seconds before the triggering event/beginning of the triggering time interval) as well as on which devices the action should take place. This type of action requires that recording has been enabled on the cameras to which the action will be linked. Being able to save video from before an event or time interval is only possible if prebuffering is enabled for the cameras in question. You enable recording and specify prebuffering settings for a camera on the *Record* tab (see "Record Tab Overview" on page 103). ***Stop action required:*** This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Stop recording. Without this stop action, recording would potentially continue indefinitely. You will also have the option of specifying further stop actions.
Start feed on <devices>	Begin video feed from camera devices to RC-E. When the feed from a device is started, video will be transferred from the device to RC-E , in which case live viewing and recording of video will be possible. **IMPORTANT:** While this type of action enables access to selected cameras' video feeds, it does not guarantee that video will be recorded, as cameras' recording settings must be specified separately. When selecting this type of action, *Manage Rule* will prompt you to specify on which devices feeds should be started. **Tip:** RC-E has a default rule ensuring that feeds are always started on all cameras. Note however, that the default rule may have been manually deactivated or modified. See Manage Rules (on page 133) for more information. ***Stop action required:*** This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Stop feed. You will also have the option of specifying further stop actions. Note that using the compulsory stop action *Stop feed* to stop the feed from a device means that video will no longer be transferred from the device to RC-E, in which case live viewing and recording of video will no longer be possible. However, a device on which the feed has been stopped will still be able to communicate with the recording server, and the feed can be started again automatically through a rule, as opposed to when the device has been manually disabled in the Management Client.
Set live frame rate on <devices>	Sets a particular frame rate to be used when displaying live video from the selected cameras, instead of the cameras' default frame rate. **Tip:** The default live frame rate of a camera is specified on the *Settings* tab (see "Settings Tab Overview" on page 106). When selecting this type of action, *Manage Rule* will prompt you to specify which frame rate to set, and on which devices.

Action	Description
	Always verify that the frame rate (number of frames per second) you specify is available on the cameras in question. ***Stop action required:*** This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Restore default live frame rate. Without this stop action, the default frame rate would potentially never be restored. You will also have the option of specifying further stop actions.
Set recording frame rate on <devices>	Sets a particular frame rate to be used when saving recorded video from the selected cameras in the database, instead of the cameras' default recording frame rate. When selecting this type of action, *Manage Rule* will prompt you to specify which recording frame rate to set, and on which cameras. Specifying recording frame rate is only possible for MJPEG, a video codec (technology for compressing and decompressing data) with which each frame is separately compressed into a JPEG image. This type of action also requires that recording has been enabled on the cameras to which the action will be linked. You enable recording for a camera on the *Record* tab (see "Record Tab Overview" on page 103). The maximum frame rate you will be able to specify will depend on the camera types in question, and on their selected image resolution. ***Stop action required:*** This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Restore default recording frame rate. Without this stop action, the default recording frame rate would potentially never be restored. You will also have the option of specifying further stop actions.
Start patrolling on <device> using <profile> with PTZ priority <priority>	Begins PTZ patrolling (the continuous moving of a camera between a number of preset positions) according to a particular patrolling profile (the exact definition of how patrolling should be carried out, including the sequence of preset positions, timing settings, etc.) for a particular PTZ camera with a particular priority. **What is Priority?**When several users on a surveillance system wish to control the same PTZ camera at the same time, conflicts may occur. PTZ priority lets you alleviate the problem by specifying a priority for use of the selected PTZ camera(s) by users/groups with the selected role. Specify a priority from *1* to *32.000*, where *1* is the lowest priority. Default PTZ priority is 3000. If your system is upgraded from an older version of RC-E , the old values (*Very Low, Low, Medium, High* and *Very High*) have been translated as follows: ▸ Very Low = 1000 ▸ Low = 2000 ▸ Medium = 3000 ▸ High = 4000 ▸ Very High = 5000 If your system is upgraded to RC-E 4.0 (or future versions), rule priority settings is a new feature. Existing rules (created without priority) automatically get priority 1. It is

Action	Description
	strongly recommended to reconsider this lowest possible priority for all affected rules. When selecting this type of action, *Manage Rule* will prompt you to select a patrolling profile. Only one patrolling profile on one device can be selected; it is not possible to select several patrolling profiles. This type of action requires that the device to which the action will be linked is a PTZ (Pan/Tilt/Zoom) device, and that at least one patrolling profile has been defined for the device. You define patrolling profiles for a PTZ camera on the *Patrolling* tab (see "PTZ Patrolling Tab (Camera Properties)" on page 80). ***Stop action required:*** This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Stop patrolling. Without this stop action, patrolling would potentially never stop. You will also have the option of specifying further stop actions.
Pause patrolling on <devices>	Pauses PTZ patrolling (the continuous moving of a camera between a number of preset positions). When selecting this type of action, *Manage Rule* will prompt you to specify the devices on which patrolling should be paused. This type of action requires that the devices to which the action will be linked are PTZ (Pan/Tilt/Zoom) devices, and that at least one patrolling profile has been defined for those devices. You define patrolling profiles for a PTZ camera on the *Patrolling* tab (see "PTZ Patrolling Tab (Camera Properties)" on page 80). ***Stop action required:*** This type of action requires one or more stop actions. Depending on how the action was triggered, the stop action may be performed either on an event or after a period of time. In one of the subsequent steps of Manage Rule, the wizard will automatically prompt you to specify the stop action: Resume patrolling. Without this stop action, patrolling would potentially pause indefinitely. You will also have the option of specifying further stop actions.
Move <device> to <preset> position with PTZ priority <priority>	Moves a particular camera to a particular preset position - however always according to priority. When selecting this type of action, *Manage Rule* will prompt you to select a preset position. Only one preset position on one camera can be selected; it is not possible to select several preset positions. If your system is upgraded to RC-E 4.0 (or future versions), rule priority settings is a new feature. Existing rules (created without priority) automatically get priority 1. It is strongly recommended to reconsider this lowest possible priority for all affected rules. This type of action requires that the devices to which the action will be linked are PTZ (Pan/Tilt/Zoom) devices, and that at least one preset position has been defined for those devices. You define preset positions for a PTZ camera on the *Presets* tab (see "PTZ Presets Tab (Camera Properties)" on page 83). ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Move to default preset on <devices> with PTZ priority <priority>	Moves one or more particular cameras to their respective default preset positions - however always according to priority. When selecting this type of action, *Manage Rule* will prompt you to select which devices the action should apply for. If your system is upgraded to RC-E 4.0 (or future versions), rule priority settings is a new feature. Existing rules (created without priority) automatically get priority 1. It is

Action	Description
	strongly recommended to reconsider this lowest possible priority for all affected rules. This type of action requires that the devices to which the action will be linked are PTZ (Pan/Tilt/Zoom) devices, and that default preset positions have been defined for those devices. You define default preset positions for a PTZ camera on the *Presets* tab (see "PTZ Presets Tab (Camera Properties)" on page 83). ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Set device output to <state>	Sets an output on a device to a particular state (activated or deactivated). When selecting this type of action, *Manage Rule* will prompt you to specify which state to set, and on which devices. This type of action requires that the devices to which the action will be linked each have at least one external output unit connected to an output port. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Create bookmark on <device>	Creates a bookmark on live streaming or recordings from a selected device. A bookmark makes it easy to retrace a certain event or period in time. Bookmark settings are controlled from the Options (on page 168) dialog. When selecting this type of action, *Manage Rule* will prompt you to specify bookmark details and select device. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Send notification to <profile>	Sends a notification, using a particular notification profile. When selecting this type of action, *Manage Rule* will prompt you to select a notification profile, and which devices to include pre-alarm images from. Only one notification profile can be selected; it is not possible to select several notification profiles. **Tip:** Even though you are only able to select a single notification profile, bear in mind that a single notification profile may contain several recipients. This type of action requires that at least one notification profile (see "Manage Notification Profiles" on page 141) has been set up. Pre-alarm images will only be included if e-mail notification is used and the *Include images* option has been enabled for the notification profile in question. **IMPORTANT:** Pre-alarm images functionality cannot coexist with edge recording (see "Record Tab Overview" on page 103). So if a camera is setup to export pre-alarm images it is not possible to enable edge recording on that camera, and vice versa. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Make new <log entry>	Generates an entry in the rule log (see "Manage Logs" on page 158). When selecting this type of action, *Manage Rule* will prompt you to specify a text for the log entry. **Tip:** When specifying the log text, you will be able to quickly insert variables, such as *$DeviceName$*, *$EventName$*, etc. into the log message wording. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either

Action	Description
	an event or after a period of time.
Start plug-in on <devices>	Starts one or more plug-ins. When selecting this type of action, *Manage Rule* will prompt you to select required plug-ins, and on which devices to start the plug-ins. This type of action requires that at one or more plug-ins are available on your system. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Stop plug-in on <devices>	Stops one or more plug-ins. When selecting this type of action, *Manage Rule* will prompt you to select required plug-ins, and on which devices to stop the plug-ins. This type of action requires that at one or more plug-ins are available on your system. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Apply new settings on <devices>	Changes device settings. When you select this type of action, *Manage Rule* will prompt you to select required devices, and you will be able to define required settings on the devices you have specified. If defining settings for more than one device, you will only be able to change settings that are available for all of the specified devices. ***Example:*** You specify that the action should be linked to Device 1 and Device 2. Device 1 has the settings A, B and C, and Device 2 has the settings B, C and D. In this case, you will only be able to change the settings that are available for both devices, namely settings B and C. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Send SNMP trap	Generates a small message which logs events on selected devices. The text of SNMP traps are auto-generated and cannot be customized. It will typically contain the source type and name of the device on which the event occurred. To configure who receives SNMP trap messages, see SNMP Support (on page 201). ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
Retrieve edge storage recordings from <devices>	Retrieves and stores edge recordings from selected devices (that support edge recording (see "Enabling and Disabling Edge Recording—Camera Only" on page 106)). Can be set to execute immediately or at a certain point in time. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time. Note that this rule is independent of the *Use edge recording if device is unavailable* setting (see "Enabling and Disabling Edge Recording—Camera Only" on page 106).
Save attached image	Ensures that when an image is received from the Images Received event (see "Events Overview" on page 128) (sent via SMTP e-mail from a camera) it is saved for future usage. In future, other events might also be able to trigger this action. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either

Action	Description
	an event or after a period of time.
Activate archiving on <archives>	Starts archiving on one or more archives. When you select this type of action, *Manage Rule* will prompt you to select required archives. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.
On <site> trigger <user-defined event>	Relevant mostly within OnSSI Federated Architecture (see "OnSSI Federated Architecture Overview" on page 173), but can also be used in a single server setup. Used for triggering a user defined event on a site - normally a remote site within a federated hierarchy. ***No compulsory stop action:*** This type of action does not require a stop action; although it will be possible to specify optional stop actions to be performed on either an event or after a period of time.

Create Typical Rules

The following is a brief introduction to examples of typical rules, what you can do with them and how they can be constructed.

Basic Rules

- ***Use Higher Live Frame Rate on Motion****:* Ensures that when motion is detected on a specific camera, RC-E will use a higher than default live frame rate for the camera, and return to using the camera's default live frame rate when motion is no longer detected. The effect is higher quality live video whenever there is motion. When the specified part of the day ends, the PTZ camera will stop patrolling.

PTZ-Related Rules

- ***Use Specific PTZ Patrolling Profile During Specific Part of Day****:* Ensures that during a specific part of the day, a PTZ (Pan/Tilt/Zoom) camera will patrol according to a specific patrolling profile (i.e. the exact definition of how patrolling should be carried out, including the sequence for moving between preset positions, timing settings, etc.). When the specified part of the day ends, the PTZ camera will stop patrolling.
- ***Use Different PTZ Patrolling Profiles for Day/Night:*** Ensures that during daytime, a PTZ camera will patrol according to a specific patrolling profile. And during nights, according to another patrolling profile.
- ***Pause PTZ Patrolling and Go to PTZ Preset on Input****:* Ensures that a specific external input is activated, a PTZ camera will pause its patrolling, move to a specific preset position, and remain at the preset position for a specific period of time, after which it will resume patrolling.

Use Higher Live Frame Rate on Motion

In this example, the camera has a default live frame rate of 10 frames per second (FPS), and the rule will increase the live frame rate to 25 FPS when applied. The effect will be a higher quality live video for as long as motion is detected on the camera.

Note that recording frame rate (the frame rate with which video sequences will be saved) is specified separately, and will not be affected by this rule.

Tip: If you want to permanently change the default frame rate for a camera, do not use a rule. Change the camera's default frame rate on the *Settings* tab (see "Settings Tab Overview" on page 106) instead.

Motion is normally detected by RC-E when video received from cameras is analyzed. This is the type of motion detection dealt with in this example. However, some cameras are— depending on configuration of the camera hardware— themselves able to detect motion. Such hardware-configurable motion detection can also be used in RC-E rules, although that is beyond the scope of this example.

Prerequisites

This rule is based on motion detection on a specific camera. Therefore, motion detection must be enabled on the camera in order for the rule to work as intended. Before creating a rule like this, always verify the following:

- Motion detection is enabled for the camera in question

Show me how to verify this...

To verify that motion detection has been enabled for a camera, expand Devices in the Management Client's Site Navigation pane, and select Cameras. This will display a list of cameras in the overview pane. Select the required camera from the list, and select the Motion tab in the Properties pane. On the Motion tab, verify that the Enable motion detection check box is selected.

Note that other settings on the *Motion* tab, such as *Sensitivity*, will determine what will be interpreted as motion. Merely enabling motion detection may thus not be sufficient to meet your requirements. Time spent on finding the best possible balance of motion detection settings under different conditions (day/night, calm/windy weather, etc.) will help you later avoid unnecessary recordings, etc.

Creating the Rule

1. In the Management Client's Site Navigation pane, expand *Rules and Events*, then right-click Rules and select *Add New Rule...*:

   Tip: Instead of right-clicking to select *Add New Rule*, you can press CTRL+N on your keyboard.

2. The *Manage Rule* wizard opens. Type a name for the new rule in the *Rule name* field.

   In this example... the rule will cover a specific camera, Camera 1. We therefore overwrite the default rule name (e.g. New Rule 001) with a descriptive name:

   Tip: Always use a descriptive name for the rule. Once you have several rules, you will find that descriptive names are a great help when identifying individual rules.

3. On Step 1 of *Manage Rule*, select the required rule type.

   In this example... we want to base the rule on an event, namely detected motion. Therefore, we select *Perform an action on <event>*. Our selection is immediately reflected in the initial rule description in the lower half of the wizard window:

4. Click the underlined items in the rule description in order to specify its exact content:

   Event link: Clicking the *event* link lets you select the event which must occur in order for the rule to apply. In order for you to get a good overview, selectable events are listed in groups according to whether they are related to plug-ins, dependent on hardware configuration, built into RC-E itself, etc.

   In this example ... we want the event to be detected motion. Motion detection events are technically related to RC-E's motion detection plug-in, so we go to the *Plug-ins* group, select the event *Motion Start*, and click *OK*:

Devices/recording server/management server link: When you have selected the required event, clicking the *devices/recording server/management server* link opens the *Select Group Members* window, which lets you specify the devices on which device the event should occur in order for the rule to apply.

> **In this example** ... the event should occur on Camera 1 in order for the rule to apply. In the *Select Group Members* window we therefore drag Camera 1 to the *Selected* list and click *OK*.

5. Click *Next* to move to step 2 of the wizard. On step 2 of the wizard, specify which time conditions should be met in order for the rule to apply.

   > **In this example** ... we simply want the rule to apply whenever motion is detected on Camera 1, regardless of time. When creating event-based rules it is possible to bypass the time conditions; we therefore want to skip step 2 entirely.

6. Click *Next* to move to step 3 of the wizard. On step 3 of the wizard, first specify which actions to perform.

   > **In this example** ... we want to set a specific live frame rate. We therefore select the action *Set live frame rate on <devices>*:

   Based on the selection of actions, the wizard automatically extends the rule description in the lower part of the wizard window.

   > **In this example** ... Based on our selection *Set live frame rate on <devices>*, the wizard automatically suggests a rule description in which the frame rate should be set on *the device on which event occurred*. The wizard furthermore prompts us to specify the required number of frames per second:

   To specify the required number of frames per second, we click the *frames per second link*, specify a frame rate of 25, and click *OK*:

   The rule description now indicates that the frame rate will be set to 25 frames per second.

7. Click *Next* to move to step 4 of the wizard. On step 4 of the wizard, select stop criteria. Stop criteria are important in many types of rules. Without a stop criterion, many actions could go on indefinitely once started.

   > **In this example** ... Without a stop criterion, the rule in this example would set the frame rate for the camera to 25 FPS indefinitely upon motion detection. Based on the elements in our rule description, the wizard therefore automatically suggests the stop criterion *Perform stop action on <event>*:

   Note that the stop criterion *No actions performed on rule end* is not available: a stop criterion must be defined for this type of rule. In the rule description, the wizard furthermore automatically suggests that the stop action is performed when motion is no longer detected on Camera 1:

   This is just what we want; we do not need to change any of the wizard's suggestions. However, we still need to define exactly which kind of stop action should take place when motion ends on Camera 1.

8. Click *Next* to move to the next step of the wizard. In this step, the wizard suggests one or more stop actions based on the previously selected start actions.

   > **In this example** ... Based on the start action *set frame rate* in our rule description, the wizard automatically suggests the stop action *restore default frame rate*. It furthermore suggests that the default frame rate should be restored immediately after the last detected motion:

   This is also just what we want; we do not need to change it, although by clicking the *immediately* link we could have specified a delay of e.g. 3 seconds.

   Your rule is by default active, meaning that once you have created it, it will be applied as soon as the rule's conditions are met. If you do not want the rule to be active straight away, clear the *Active* check box in the top part of the *Manage Rule* window:

   Tip: You can always activate/deactivate the rule later.

9. Click *Finish*. This will add your new rule to the list of rules.

Use Specific PTZ Patrolling Profile During Specific Part of Day

Tip: When patrolling stops, you can—if needed—get the PTZ camera to start patrolling immediately after according to another patrolling profile (see "Use Different PTZ Patrolling Profiles for Day/Night" on page 121).

Prerequisites

When a PTZ camera patrols according to a patrolling profile, it continuously moves between different preset positions. Therefore, the required preset positions and at least one patrolling scheme must be defined for the PTZ camera in question. Before creating a rule like this, always verify the following:

- The camera in question is a PTZ camera
- At least two preset positions are defined for the camera

  How to define preset positions...

  To define preset positions for a PTZ camera, expand Devices in the Management Client's Site Navigation pane (see "Panes Overview" on page 36) and select Cameras. In the overview pane (see "Panes Overview" on page 36), select the required PTZ camera from the list, then select the Presets tab in the properties pane (see "Panes Overview" on page 36). For descriptions of the exact functionality of the Presets tab, see Preset Positions (see "PTZ Presets Tab (Camera Properties)" on page 83).

- At least one patrolling profile is defined for the camera

  How to define a patrolling profile...

  To define patrolling profiles for a PTZ camera, expand Devices in the Management Client's Site Navigation pane (see "Panes Overview" on page 36) and select Cameras. In the overview pane (see "Panes Overview" on page 36), select the required PTZ camera from the list, then select the Patrolling tab in the properties pane (see "Panes Overview" on page 36). For descriptions of the exact functionality of the *Patrolling* tab, see Patrolling (see "PTZ Patrolling Tab (Camera Properties)" on page 80).

Creating the Rule

1. In the Management Client's Site Navigation pane, expand *Rules and Events*, then right-click Rules and select *Add New Rule...*:

   Tip: Instead of right-clicking to select *Add New Rule*, you can press CTRL+N on your keyboard.

2. The *Manage Rule* wizard opens. Type a name for the new rule in the *Rule name* field.

   In this example... the rule will only cover a specific camera (simply called *PTZ Camera*) and how it should patrol on Saturday afternoons. We therefore overwrite the default rule name (e.g. *New Rule 001*) with a descriptive name:

   Tip: Always use a descriptive name for the rule. Once you have several rules, you will find that descriptive names are a great help when identifying individual rules.

3. On Step 1 of *Manage Rule*, select the required rule type.

   In this example... we want to base the rule on a time period. Therefore, we select *Perform an action in a time interval*:

   Click *Next* to move to the next step of the wizard.

4. On the wizard's next step, specify which time conditions should be met in order for the rule to apply.

   In this example... we want the rule to apply between 1:00 and 8:00 on Saturdays, so two time conditions are required: one which specifies use of a start time and end time, and one which specifies use on a particular day of the week. We therefore select *Within the time period <start time> to <end time>* and *Day of week is <day>*:

   Our selection is immediately reflected in the initial rule description in the lower half of the wizard window:

   Tip: If we had previously created a suitable time profile covering the required period of time, we could have just selected the time condition Within selected time in *<time profile>*, then pointed to the time profile in question. Read more about time profiles under Managing Time Profiles (see "Manage Time Profiles" on page 138).

5. Click the underlined items in the rule description in order to specify its exact content:

   start time: Clicking the start time link lets you specify required start time.

   In this example ... we want the start time to be one o'clock in the afternoon, so we specify 1:00, and click OK:

   end time: The *end time* link works just like the *start time* link. We specify 8:00.

   days: Clicking the *days* link lets you specify required days of the week.

   In this example ... our rule should only apply on Saturdays, so we select *Saturday*, and click *OK*:

   Click *Next* to move to step 3 of the wizard.

6. On step 3 of the wizard, first specify which actions to perform.

   In this example ... we want to start patrolling according to a specific patrolling profile. We therefore select the action *Start patrolling on <device> using <profile> with PTZ priority <priority>*:

   Based on the selection of actions, the wizard automatically extends the rule description in the lower part of the wizard window.

   In this example... Based on our selection *Start patrolling on <device> using <profile> with PTZ priority <priority>*, the wizard automatically prompts us to specify the required camera, patrolling profile and its priority (see "Actions and Stop Actions Overview" on page 110):

   We click the *device* link, expand the relevant camera folder, select the required camera, and click *OK*:

   Next we click the *profile* link, select the required patrolling profile from our list of previously defined patrolling profiles, and click *OK*:

   Finally, we click the *priority* link to set the priority (see "Actions and Stop Actions Overview" on page 110) of the patrolling profile.

   By doing this, we have further specified the content of the wizard's rule description.

   Click *Next* to move to step 4 of the wizard.

7. On step 4 of the wizard, select stop criteria. Stop criteria are important in many types of rules. Without a stop criterion, many actions could go on indefinitely once started.

   In this example... Without a stop criterion, the rule in this example would start patrolling within the specified time period, but never stop it. Based on the elements in our rule description, the wizard therefore automatically suggests the stop criterion *Perform stop action when time interval ends*:

Note that the stop criterion *No actions performed on rule end* is not available: a stop criterion must be defined for this type of rule. We still need to define exactly which kind of stop action should take place when the time period ends.

Click *Next* to move to the next step of the wizard.

8. In this step, the wizard suggests one or more stop actions based on the previously selected start actions.

   In this example ... Based on the start action start patrolling in our rule description, the wizard automatically suggests the stop action *Stop patrolling*. It furthermore suggests that patrolling is stopped immediately when the time period ends:

   This is just what we want; we do not need to change it, although by clicking the *immediately* link we could have specified a delay of e.g. 60 seconds.

   Your rule is by default active, meaning that once you have created it, it will be applied as soon as the rule's conditions are met. If you do not want the rule to be active straight away, clear the *Active* check box in the top part of the *Manage Rule* window:

   Tip: You can always activate/deactivate the rule later.

9. Click *Finish*. This will add your new rule to the list of rules:

Use Different PTZ Patrolling Profiles for Day/Night

In this example, *daytime* is defined by a time profile covering the period between 08.00 and 20.00 on all days of the week and *nights* are defined as periods not covered by the *daytime* time profile. This requires two near-identical rules; one for each patrolling profile. When you have created the first rule, you can make a copy of it, and quickly create the second rule based on the copy. Both rules are covered in this example.

Prerequisites

This rule is based on a PTZ camera being able to patrol according to two different patrolling profiles, and a time profile being used to determine which patrolling profile should be used. Before creating a rule like this, always verify the following:

- You have specified a time profile covering at least one of the time periods you want to differentiate between. You could specify time profiles covering both time periods, but it will not be necessary since rules can be set up to apply *within* as well as outside a time profile.

  How to specify a time profile...

  To specify a time profile, expand *Rules and Events* in the Management Client's Site Navigation pane (see "Panes Overview" on page 36), then select Time Profiles. The *Time Profiles* list will appear. In the *Time Profiles* list, right-click Time Profiles, and select Add Time Profile... For detailed information about specifying time profiles, see Managing Time Profiles (see "Manage Time Profiles" on page 138).

- The camera in question is a PTZ camera.

- Preset positions and at least two patrolling profiles are defined for the camera.

  How to define preset positions and patrolling profiles...

  When a PTZ camera patrols according to a patrolling profile, it moves between a number of preset positions. Thus, before you able to define patrolling profiles for a PTZ camera, the preset positions required for the patrolling profiles must be defined.

  To define preset positions for a PTZ camera, expand *Devices* in the Management Client's Site Navigation pane (see "Panes Overview" on page 36) and select *Cameras*. This will display a list of cameras in the

overview pane (see "Panes Overview" on page 36). Select the required PTZ camera from the list, and select the Presets tab in the properties pane (see "Panes Overview" on page 36). For details of how to define preset positions on the *Presets* tab, see Preset Positions (see "PTZ Presets Tab (Camera Properties)" on page 83).

Once you have defined the required preset positions, patrolling profiles for the PTZ camera are defined on the neighboring *Patrolling* tab. For details of how to define patrolling profiles on the *Patrolling* tab, see Patrolling (see "PTZ Patrolling Tab (Camera Properties)" on page 80).

Creating the First Rule; Patrolling During Daytime

1. In the Management Client's Site Navigation pane, expand *Rules and Events*, then right-click Rules and select *Add New Rule...*:

   Tip: Instead of right-clicking to select *Add New Rule*, you can press CTRL+N on your keyboard.

2. The *Manage Rule* wizard opens. Type a name for the new rule in the *Rule name* field.

   In this example...the rule will cover a specific camera and how it should patrol during daytime. We therefore overwrite the default rule name (e.g. *New Rule 001*) with a descriptive name:

   Tip: Always use a descriptive name for the rule. Once you have several rules, you will find that descriptive names are a great help when identifying individual rules.

3. On Step 1 of *Manage Rule*, select the required rule type.

   In this example...we want to base the rule on a time period. Therefore, we select *Perform an action in a time interval*:

   Click *Next* to go to step 2 of the wizard.

4. On step 2 of the wizard, specify which time conditions should be met in order for the rule to apply.

   In this example... we want the rule to apply within a specific time profile, so we select the time condition *Within selected time in <time profile>*:

   Based on our selection, the wizard prompts us to specify the required time profile in the rule description:

   Click the underlined item to specify the exact content of the rule description.

   In this example... we click the time *profile* link, select the time profile *Daytime*, and click *OK*:

   The rule description now reflects our selection:

   Click *Next* to move to step 3 of the wizard.

5. On step 3 of the wizard, first specify which actions to perform.

   In this example...we want patrolling according to a specific patrolling profile. We therefore select the action *Start patrolling on <device> using <profile> with PTZ priority <priority>*:

   Based on the selection of actions, the wizard extends the rule description, and prompts us to specify the required device, patrolling profile and its priority (see "Actions and Stop Actions Overview" on page 110):

   Click the underlined items in the extension of the rule description in order to specify their exact contents:

   In this example... we first click the *device* link and in the *Select device* dialog opening we select a device and click *OK*:

   Then we click the *profile* link and select a patrolling profile in the dialog opening and then click OK.

Finally, click the *priority* link to set the priority (see "Actions and Stop Actions Overview" on page 110) of the patrolling profile.

The rule description now reflects our selection:

Click *Next* to move to step 4 of the wizard.

6. On step 4 of the wizard, select stop criteria.

   Stop criteria are important in many types of rules. Without a stop criterion, many actions could go on indefinitely once started.

   In this example...Without a stop criterion, the rule in this example would make the PTZ camera start patrolling according to the selected patrolling profile, but it would never stop. Based on the elements in our rule description, we therefore must select a stop criterion. Since our rule is triggered when a time period starts, the wizard automatically suggests that stop action is performed when the time period ends:

   The suggestion is also reflected in the rule description. However, we still need to specify exactly which stop action we want performed.

   Click *Next* to move to the next step of the wizard.

7. In this step, the wizard suggests one or more stop actions based on the previously selected start actions.

   In this example...Based on the start action *start patrolling* in our rule description, the wizard automatically suggests the stop action *stop patrolling*. It furthermore suggests that patrolling is stopped immediately when the time period ends:

   This is exactly what we want; we do not need to change it.

   Your rule is by default active, meaning that once you have created it, it will be applied as soon as the rule's conditions are met.

   If you do not want the rule to be active straight away, clear the *Active* check box in the top part of the *Manage Rule* window:

   Tip: You can always activate/deactivate the rule later.

8. Click *Finish*. This will add your new rule to the list of rules:

Creating the Second Rule; Patrolling During Night-time

Tip: You do not have to create the second rule from scratch; you can make a copy of the first rule, then change it. To copy a rule, select the rule in the *Rules* list, right-click, and select *Copy Rule*... This will open *Manage Rule*, which will display an editable copy of the rule.

1. Copy the first rule, then make the following changes to the rule:

   - Change the rule name so it better describes the new rule, for example to *PTZ Camera Nighttime Patrolling*.
   - On the time conditions selection step, select that the rule should apply not within but *outside* the time profile.
   - In the rule description, click the link in the sentence *Start patrolling on ...*, and select a patrolling profile matching your nighttime requirements rather than your daytime requirements.

2. Click *Finish*.

Pause PTZ Patrolling and Go to PTZ Preset on Input

In this example, we assume that patrolling has already been set up for the PTZ camera, and that the external input unit is a door sensor connected to an input port on a device on the RC-E system: When the door sensor is activated, the PTZ camera will pause patrolling, move to a preset position covering the door area, remain at the preset position for 15 seconds, then resume patrolling.

Prerequisites

This rule is based on an input being activated, and on a patrolling PTZ camera moving to a specific preset position. Therefore, an external input unit must be available, i.e. connected to the input port of a device on the RC-E system. Furthermore, the preset position to which the PTZ camera should move when the rule is applied must have been defined. Before creating a rule like this, always verify the following:

- An external input unit is successfully connected to an input port on a device, and the states of the input unit (activated/deactivated) work as required.
- The camera in question is a PTZ camera with the required preset positions and patrolling defined.

  How to define preset positions and patrolling profiles...

  When a PTZ camera patrols according to a patrolling profile, it moves between a number of preset positions. Thus, before you able to define patrolling profiles for a PTZ camera, the preset positions required for the patrolling profiles must be defined.

  To define preset positions for a PTZ camera, expand *Devices* in the Management Client's Site Navigation pane (see "Panes Overview" on page 36) and select *Cameras*. This will display a list of cameras in the overview pane (see "Panes Overview" on page 36). Select the required PTZ camera from the list, and select the Presets tab in the properties pane (see "Panes Overview" on page 36). For details of how to define preset positions on the *Presets* tab, see Preset Positions (see "PTZ Presets Tab (Camera Properties)" on page 83).

  Once you have defined the required preset positions, patrolling profiles for the PTZ camera are defined on the neighboring *Patrolling* tab. For details of how to define patrolling profiles on the *Patrolling* tab, see Patrolling (see "PTZ Patrolling Tab (Camera Properties)" on page 80).

Creating the Rule

1. In the Management Client's Site Navigation pane, expand *Rules and Events*, then right-click Rules and select *Add New Rule...*:

   Tip: Instead of right-clicking to select *Add New Rule*, you can press CTRL+N on your keyboard.

2. The *Manage Rule* wizard opens. Type a name for the new rule in the *Rule name* field.

   In this example... the rule will cover a specific camera (*simply called PTZ Camera*) and how it should behave upon an activated input. We therefore overwrite the default rule name (e.g. *New Rule 001*) with a descriptive name:

   Tip: Always use a descriptive name for the rule. Once you have several rules, you will find that descriptive names are a great help when identifying individual rules.

3. On Step 1 of *Manage Rule*, select the required rule type.

   In this example... we want to base the rule on an event. Therefore, we select *Perform an action* on <*event*>. Our selection is immediately reflected in the initial rule description in the lower half or the wizard window.

   Click the underlined items in the rule description in order to specify its exact content:

Event link: Clicking the *event* link lets you select the event which must occur in order for the rule to apply. In order for you to get a good overview, selectable events are listed in groups according to whether they are related to plug-ins, dependent on hardware configuration, built into RC-E itself, etc.

In this example...we want the event to be activated input. Input comes from— and is configured on— separate hardware rather than on RC-E itself, so we go to the *Hardware Configurabl*e group, select the event *Input Activated*, and click *OK*:

Devices/recording server/management server link: When you have selected the required event, clicking the *devices/recording server/management server* link opens the *Select Devices and Groups* window, which lets you specify the devices on which the event should occur in order for the rule to apply.

In this example... the event should occur on an input called *Back Door Sensor* in order for the rule to apply. In the *Select Devices and Groups* window we therefore drag the input *Back Door Sensor* to the *Selected* list and click *OK*. By doing this we have specified the exact content of the first part of the wizard's rule description.

Click *Next* to move to step 2 of the wizard.

4. On step 2 of the wizard, specify which time conditions should be met in order for the rule to apply.

   In this example...we simply want the rule to apply whenever input is activated on the back door sensor, regardless of time. When creating event-based rules it is possible to bypass the time conditions; we therefore want to skip the wizard's step 2 entirely.

   Click *Next* to move to step 3 of the wizard.

5. On step 3 of the wizard, first specify which actions to perform.

   In this example...we want to two things to happen: patrolling should pause, and the PTZ camera should move to a specific preset position with a specific priority (see "Actions and Stop Actions Overview" on page 110). We therefore select the actions Pause patrolling on *<devices>* and *Move <device> to <preset> position with PTZ priority <priority>*.

   Based on the selection of actions, the wizard automatically extends the rule description in the lower part of the wizard window.

   In this example...Based on our selections Pause patrolling on *<devices>* and *Move <device> to <preset> position with PTZ priority <priority>* the wizard automatically suggests an extension to the existing rule description:

6. Click the underlined items in the extension of the rule description in order to specify its exact content:

   devices: Clicking the devices link lets you select the devices on which patrolling should be paused. Only PTZ cameras will be selectable.

   In this example...patrolling should be paused on our PTZ camera. In the *Select Group Members* window we therefore drag *PTZ Camera to the Selected* list and click *OK*.

   device: Clicking the *device* link lets you select to move another device than the device(s) on which patrolling was paused. You are also able to select to move the device on which patrolling was paused.

   In this example...we select to move the same PTZ camera on which patrolling was paused, and click OK:

   preset: Clicking the *preset* link lets you select which preset position the PTZ camera should move to. You will be able to select from a list of preset positions defined for the PTZ camera you selected before.

   In this example...we select a preset position called *Back Door*, and click *OK*:

   immediately: The wizard automatically suggests that the camera moves to the preset position *immediately* after it has paused patrolling. Clicking the immediately link lets you specify a delay, if required.

priority: Clicking the *priority* link lets you specify the priority (see "Actions and Stop Actions Overview" on page 110) of the camera position.

In this example...the wizard's suggestion *immediately* suits us fine, so we simply leave it as it is.

The rule description now indicates which camera will pause patrolling, which preset position it will move to, and how soon:

Click *Next* to move to step 4 of the wizard.

7. On step 4 of the wizard, select stop criteria.

   Stop criteria are important in many types of rules. Without a stop criterion, many actions could go on indefinitely once started.

   In this example...Without a stop criterion, the rule in this example would make the camera pause patrolling, then move to the preset position and remain there indefinitely. Based on the elements in our rule description, we therefore **must** select a stop criterion.

   Since our rule is triggered by an event, the wizard automatically suggests that we base our stop action on an event as well. In the rule description, the wizard even suggests that the stop action is performed when input is deactivated on the back door sensor. However, we want something different, so we select *Perform stop action after <time>*:

   In the rule description, the wizard now prompts us to specify the required time.

   We click the *time* link, specify 15 seconds, and click *OK*:

   The rule description now indicates the 15 seconds selected.

   Based on the start action *pause patrolling* in our rule description, the wizard automatically suggests the stop action *resume patrolling*. It furthermore suggests that patrolling is resumed immediately after the 15 second pause:

   This is exactly what we want; we do not need to change it, although by clicking the *immediately* link we could have specified a delay of e.g. 3 seconds.

   Your rule is by default active, meaning that once you have created it, it will be applied as soon as the rule's conditions are met. If you do not want the rule to be active straight away, clear the *Active* check box in the top part of the *Manage Rule* window:

   Tip: You can always activate/deactivate the rule later.

8. Click *Finish*. This will add your new rule to the list of rules:

Default Rules

OnSSI RC-E comes with a number of default rules, ensuring that basic features work without any user intervention being required.

IMPORTANT: Like other rules, default rules can be deactivated and/or modified as required. The fact that default rules are present does therefore not in itself guarantee that your RC-E system will work. Nor does it guarantee that video feeds or audio feeds will automatically be fed to the RC-E system, as the default rules may subsequently have been deactivated or modified.

Default Start Feed Rule

Ensures that video feeds from all connected cameras are automatically fed to the RC-E system.

IMPORTANT: While the default rule enables access to connected cameras' video feeds immediately upon installing the system, it does not guarantee that video will be recorded, as cameras' recording settings must be specified separately.

In case you accidentally delete the default start feed rule, you can recreate it with the following content:

```
Perform an action in a time interval always start feed on All Cameras
Perform an action when time interval ends stop feed immediately
```

Default Start Audio Feed Rule

Ensures that audio feeds from all connected microphones and speakers are automatically fed to the RC-E system.

IMPORTANT: While the default rule enables access to connected microphones' and speakers' audio feeds immediately upon installing the system, it does not guarantee that audio will be recorded (see "Record Tab Overview" on page 103), as recording settings must be specified separately.

In case you accidentally delete the default start audio feed rule, you can recreate it with the following content:

```
Perform an action in a time interval always start feed on All Microphones, All Speakers
Perform an action when time interval ends stop feed immediately
```

Default Record on Motion Rule

Ensures that as long as motion is detected in video from cameras, the video will be recorded, provided recording is enabled (see "Record Tab Overview" on page 103) for the cameras in question (recording is by default enabled).

IMPORTANT: While the default rule specifies recording based on detected motion, it does not guarantee that video will be recorded, as individual cameras' recording may have been disabled for one or more cameras. Even when recording is enabled, bear in mind that the quality of recordings may be affected by individual camera's recording settings.

In case you accidentally delete the default record on motion rule, you can recreate it with the following content:

```
Perform an action on Motion Started from All Cameras start recording 3 seconds before on the device on which event occurred
Perform stop action on Motion Stopped from All Cameras stop recording 3 seconds after
```

Default Goto Preset when PTZ Is Done Rule

Ensures that PTZ (Pan/Tilt/zoom) cameras will go to their respective default preset positions after they have been operated manually.

IMPORTANT: This rule is by default not enabled. Even when the rule is enabled, you must have defined default preset positions for the required PTZ cameras in order for the rule to work; you do this on the *Presets* tab (see "PTZ Presets Tab (Camera Properties)" on page 83).

In case you accidentally delete the default goto preset when PTZ is done rule, you can recreate it with the following content:

```
Perform an action on PTZ Manual Session Stopped from All Cameras
Move immediately to default preset on the device on which event occurred
```

Events Overview

When creating an event-based rule in the *Manage Rule* wizard (see Manage Rules (on page 133)), you are able to select between a number of different events.

In order for you to get a good overview, selectable events are listed in groups according to whether they are:

Devices

Dependent on hardware configuration

Event	Description
Events Dependent on Hardware Configuration The configuration on which these events depend may only be possible on some hardware. For example, only selected cameras may be able to detect tampering or temperature changes.	
Audio Falling	Occurs when the audio signal on an audio-enabled device is falling. For exact information about what constitutes a falling and a rising signal respectively, refer to documentation for the device in question. This type of event requires that at least one device on your system has an audio unit connected. The event will not work until configured on the hardware itself.
Audio Passing	Occurs when the state of an audio-enabled device is changed, regardless of which state the device is changed to. This type of event requires that at least one device on your system has an audio unit connected. The event will not work until configured on the hardware itself.
Audio Rising	Occurs when the audio signal on an audio-enabled device is rising. For exact information about what constitutes a falling and a rising signal respectively, refer to documentation for the device in question. This type of event requires that at least one device on your system has an audio unit connected. The event will not work until configured on the hardware itself.
Images Received	Occurs when pre-alarm images are received from a camera (using the *Include Images* option in Send notification to <profile> action (see "Actions and Stop Actions Overview" on page 110)). Pre-alarm images are available for selected cameras only; such cameras are capable of sending of one or more single still images from immediately before an event took place to the surveillance system via SMTP e-mail. This type of event requires that at least one camera on your system supports pre-alarm images. The event will not work until configured on the hardware itself. **IMPORTANT:** Pre-alarm images functionality cannot coexist with edge recording (see "Record Tab Overview" on page 103). So if a camera is setup to export pre-alarm images it is not possible to enable edge recording on that camera, and vice versa. **Tip :** Consider using prebuffering, defined on the Record tab (see "Record Tab Overview" on page 103), as an alternative to pre-alarm images.
Input Activated	Occurs when an external input unit connected to an input port on a device is activated. This type of event requires that at least one device on your system has an external input unit connected to an input port. The event will not work until configured on the hardware itself.

Event	Description
Input Changed	Occurs when the state of an external input unit connected to an input port on a device is changed, regardless of which state the external input unit is changed to. This type of event requires that at least one device on your system has an external input unit connected to an input port. The event will not work until configured on the hardware itself.
Input Deactivated	Occurs when an external input unit connected to an input port on a device is deactivated. This type of event requires that at least one device on your system has an external input unit connected to an input port. The event will not work until configured on the hardware itself.
Motion Started (HW)	Occurs when a camera detects motion in its video stream. In addition to RC-E's motion detection, some cameras are— depending on configuration of the camera hardware— themselves able to detect motion. Such camera-detected motion detection can also be used in RC-E rules. The event will not work until configured on the camera hardware itself. Exact use of camera-based motion detection depends on the configuration of the cameras in question.
Motion Stopped (HW)	Occurs when a camera no longer detects motion in its video stream. See also the description of the *Motion Started* event earlier. The event will not work until configured on the camera hardware itself. Exact use of camera-based motion detection depends on the configuration of the cameras in question.
Tampering	Occurs when a device detects that it is being tampered with. The event will not work until configured on the hardware itself. Exact use of tampering detection depends on the configuration of the devices in question.
Temperature	Occurs when a device detects a temperature change, that a certain temperature is exceeded, or similar. The event will not work until configured on the hardware itself. Exact use of temperature detection depends on the configuration of the devices in question.
Video Lost	Occurs when a device detects that a video signal is lost. The event will not work until configured on the hardware itself. Exact use of this type of detection depends on the configuration of the devices in question.

Related to plug-ins

Event	Description
Events Related to Plug-ins	

Event	Description
Motion Started	Occurs when RC-E detects motion in video received from cameras. This type of event requires that RC-E's motion detection is enabled for the cameras to which the event will be linked. Exactly what constitutes motion depends on the motion detection settings specified for individual cameras in RC-E. In addition to RC-E's motion detection, some cameras are— depending on configuration of the camera hardware— themselves able to detect motion. Such camera-detected motion detection can also be used in RC-E rules. Such events are called *Hardware Configurable*, as they do not work until configured on the camera hardware itself. See Events dependent on hardware configuration (see man_rul_Events_Overview.htm#EventsDependentonHardwareConfiguration - man_rul_Events_Overview.htm#EventsDependentonHardwareConfiguration).
Motion Stopped	Occurs when motion is no longer detected in received video. See also the description of the *Motion Started* event.

Predefined events (related to devices)

Event	Description
Predefined Events	
Communication Error	Occurs when a connection to a device is lost; or when an attempt is made to communicate with a device, and the attempt is unsuccessful.
Communication Started	Occurs when communication with a device is successfully established.
Communication Stopped	Occurs when communication with a device is successfully stopped.
Feed Overflow Started	Feed overflow (a.k.a. Media overflow) occurs when a recording server is unable to process received video as quickly as specified in the configuration and therefore is forced to discard some images. If the server is healthy, feed overflow usually happens because of slow disk writes. It can be resolved either by reducing the amount of data written, or by improving the storage system's performance. Reduce the amount of written data by reducing frame rates, resolution or image quality on your cameras. This will in general degrade recording quality. If you are not interested in that, instead improve your storage system's performance by installing extra drives to share the load or by installing faster disks or controllers. **Tip :** This rare event can be used for triggering actions that will help you avoid the problem, e.g. for lowering the recording frame rate.
Feed Overflow Stopped	Occurs when feed overflow (see description of the *Feed Overflow Started* event) ends.
Live Client Feed Requested	Occurs when a user of the Ocularis Client requests a live stream from a device. The event occurs upon the request— even if the client user's request subsequently turns out to be unsuccessful, for example because the client user does not have the rights required for viewing the requested live feed or because the feed is for some reason stopped.
Output Activated	Occurs when an external output unit connected to an output port on a device is activated. This type of event requires that at least one device on your system has an external input unit connected to an output port.
Output Changed	Occurs when the state of an external output unit connected to an output port on a device is changed, regardless of which state the external input unit is changed to.

Event	Description
	This type of event requires that at least one device on your system has an external input unit connected to an output port.
Output Deactivated	Occurs when an external output unit connected to an output port on a device is deactivated. This type of event requires that at least one device on your system has an external input unit connected to an output port.
Live Client Feed Terminated	Occurs when a user of the Ocularis Client no longer requests a live stream from a device.
Manual PTZ Session Started	Occurs when a manually operated PTZ session (as opposed to a PTZ session based on scheduled patrolling or automatically triggered by an event) is started on a camera. This type of event requires that the cameras to which the event will be linked are PTZ (Pan/Tilt/Zoom) cameras.
Manual PTZ Session Stopped	Occurs when a manually operated PTZ session (as opposed to a PTZ session based on scheduled patrolling or automatically triggered by an event) is stopped on a camera. This type of event requires that the cameras to which the event will be linked are PTZ (Pan/Tilt/Zoom) cameras.
Recording Started	Occurs when recording is started.
Recording Stopped	Occurs when recording is stopped.
Settings Changed	Occurs when settings on a device are successfully changed.
Settings Changed Error	Occurs when an attempt is made to change settings on a device, and the attempt is unsuccessful.

External Events

User-defined events

Event	Description
User-defined Events	
A number of events custom made to suit your system may also be selectable. Such user-defined events can be used for: • Making it possible for end users to manually trigger events while viewing live video in the Ocularis Client. • Countless other purposes. For example, you may create user-defined events which will occur if a particular type of data is received from a device. For information about how to define user-defined events in the Management Client, see Managing User-defined Events (see "Manage User-defined Events" on page 143).	

Related to recording servers

Event	Description
Events Related to Recording Servers	
Archive Available	Occurs when an archive (see "About Storage and Archiving" on page 56) for a recording server becomes available after having been unavailable (see *Archive Unavailable* next).
Archive Unavailable	Occurs when an archive (see "About Storage and Archiving" on page 56) for a recording server becomes unavailable, for example if the connection to an archive located on a network drive is lost. When this is the case, it will not be possible to archive recordings. You can use the event to, for example, trigger a notification profile so an e-mail notification is automatically sent to relevant people in your organization.
Archive Not Finished	Occurs when an archive (see "About Storage and Archiving" on page 56) for a recording server is not finished with the last archiving round when the next is scheduled to start.
Database Disk Full	Occurs when a database disk is full. A database disk is considered to be full when there is less than 500 MB of space is left on the disk: In order to prevent operating system failures due to insufficient disk space, the oldest records in the database will automatically be deleted for all cameras recording on the disk in question when less than 500 MB of space is left on the disk containing the database, regardless of any time or size limits specified for the database. This will help ensure that at least 500 MB of disk space will be available for operating system use.
Database Full - Auto Archive	Occurs when an archive (see "About Storage and Archiving" on page 56) for a recording server is full and needs to auto-archive to an archive in the hierarchy.
Database Repair	Occurs if a database becomes corrupted, in which case RC-E will automatically attempt two different database repair methods: a fast repair and a thorough repair.
Database Storage Area Available	Occurs when a storage area (see "About Storage and Archiving" on page 56) for a recording server becomes available after having been unavailable (see *Database Storage Area Unavailable* next). You can, for example, use the event to start recording if it has been stopped by a *Database Storage Area Unavailable* event (see next).

Event	Description
Database Storage Area Unavailable	Occurs when a storage area (see "About Storage and Archiving" on page 56) for a recording server becomes unavailable, for example if the connection to a storage area located on a network drive is lost. When this is the case, it will not be possible to store recordings. You can use the event to, for example, stop recording and trigger a notification profile (see "Manage Notification Profiles" on page 141) so an e-mail notification is automatically sent to relevant people in your organization.
Failover Started	Occurs when a failover server (see "Manage Failover Servers" on page 192) takes over from a recording server. A failover server is a spare recording server which can take over if a regular recording server becomes unavailable.
Failover Stopped	Occurs when a recording server becomes available again, and is able to take over from a failover server (see "Manage Failover Servers" on page 192).

Manage Rules

are a central element in RC-E. The behavior of an RC-E surveillance system is to a very large extent determined by rules. Rules determine highly important settings, such as when cameras should record, when PTZ (Pan/Tilt/Zoom) cameras should patrol, when notifications should be sent, etc.

You create and manage rules in the Management Client.

1. In the Management Client's *Navigation* pane, expand the *Rules and Events* folder, then select *Rules*. In the overview pane (see "Panes Overview" on page 36), a *Rules* list, providing an overview of all existing rules in your system, will appear.

2. In needed, create, edit, copy and/or validate rules from the list, see below. See also Create Typical Rules (on page 116) for a complete step-by-step guide to creating often required rules or see Default Rules (on page 126) to learn about the rules already default in RC-E.

What You Can Do with Rules

In short, rules specify actions which should be carried out under particular conditions. Example: When motion is detected (condition), a camera should begin recording (action).

The following are *examples* of what you can do with rules:

- Start and stop recording
- Set non-default live frame rate
- Set non-default recording frame rate
- Start and stop PTZ patrolling
- Pause and resume PTZ patrolling
- Move PTZ cameras to specific positions
- Set output to activated/deactivated state
- Send notifications via e-mail
- Generate log entries

- Generate events
- Apply new device settings, for example a different resolution on a camera
- Start and stop plug-ins
- Start and stop feeds from devices

How is stopping the feed from a device different from manually disabling the device? Stopping a device means that video will no longer be transferred from the device to RC-E, in which case neither live viewing nor recording will be possible. However, a device on which the feed has been stopped will still be able to communicate with the recording server, and the feed from device can be started automatically through a rule, as opposed to when the device is manually disabled in the Management Client.

IMPORTANT: Some rule content may require that certain features are enabled for the devices in question. For example, a rule specifying that a camera should record will not work as intended if recording is not enabled for the camera in question. Before creating a rule it is therefore highly recommended that you verify that the devices involved will be able to perform as intended. For a number of typically required rules, such prerequisites are described in Create Typical Rules (on page 116).

How a Rule Is Triggered

Rules can be triggered by two types of conditions:

- ***Events*:** When events occur on the surveillance system (for example when motion is detected, when the system receives input from external sensors, etc.)
- ***Time*:** When specific periods of time are entered (for example *Thursday 16th August 2007 from 07.00 to 07.59*, or *every Saturday and Sunday*)

What You Can Cover in a Rule

Your exact number of options depends on the type of rule you want to create, and on the number of devices available on your system.

Rules, however, provide a high degree of flexibility: You are able to combine event and time conditions, you are able to specify several actions in a single rule, and very often you are able to create rules covering several or all of the devices on your system.

You can make your rules as simple or complex as required. For example, you can create very simple time-based rules:

> **Example Very Simple Time-Based Rule:** *On Mondays between 08.30 and 11.30 (time condition), Camera 1 and Camera 2 should start recording (action) when the time period begins and stop recording (stop action) when* the time *period ends.*

And you can create very simple event-based rules, involving events on one device only:

> **Example Very Simple Event-Based Rule:** *When motion is detected (event condition) on Camera 1, Camera 1 should start recording (action) immediately, then stop recording (stop action) after 10 seconds.*

However, even though an event-based rule is activated by an event on one device, you can specify that actions should take place on one or more other devices.

> **Example Rule Involving Several Devices:** *When motion is detected (event condition) on Camera 1, Camera 2 should start recording (action) immediately, and the siren connected to Output 3 should sound (action) immediately; then, after 60 seconds, Camera 2 should stop recording (stop action), and the siren connected to Output 3 should stop sounding (stop action).*

You can of course also combine events and scheduled times in a rule:

Example Rule Combining Time, Events, and Devices: *When motion is detected (event condition) on Camera 1, and the day of the week is Saturday or Sunday (time condition), Camera 1 and Camera 2 should start recording (action) immediately, and a notification should be sent to the security manager (action); then, 5 seconds after motion is no longer detected on Camera 1 or Camera 2, the 2 cameras should stop recording (stop action).*

The required complexity of rules will vary from organization to organization: Some may require only a number of simple rules; some may require a mix of simple and complex rules.

Create Many Simple or a Few Complex Rules?

Depending on your organization's requirements, it is often a good idea to create many simple rules rather than a few complex rules.

Even though this will lead to you having more rules, it will generally make it much easier for you to maintain an overview of what your rules do.

Keeping your rules simple also means that you will have much more flexibility when it comes to deactivating/activating individual rule elements— with simple rules, you can deactivate/activate entire rules when required.

Default Rules

OnSSI RC-E comes with a number of default rules, ensuring that basic features work without any user intervention being required. See Default Rules (on page 126).

Creating a New Rule

When you create rules, you will be guided by the wizard *Manage Rule* which provides a highly intuitive approach. It helps you stay focused by listing only relevant options. It ensures that a rule will not contain missing elements. And finally, based on your rule's content, it automatically suggests suitable stop actions (i.e. what should take place when the rule no longer applies), ensuring that you will not unintentionally create a never-ending rule.

1. In the Overview pane (see "Panes Overview" on page 36), right-click the *Rules* item, and select *Add Rule...*:

   Tip: Instead of right-clicking to select *Add Rule*, you can press CTRL+N on your keyboard.

   This will open the wizard *Manage Rule*.

   The wizard will guide you through the process of specifying the content of your rule. The wizard makes the process interactive, yet intuitive: based on your main selections, it will ask you to specify your exact requirements for the rule.

2. Begin by specifying a name (compulsory) and a description (optional) of the new rule in the *Name* and *Description* fields respectively.

   Tip: Always use a descriptive name for the rule. Once you have several rules, you will find that descriptive names are a great help when identifying individual rules.

3. Then select the required type of condition for the rule: either a rule which performs one or more actions when a particular event occurs, or a rule which performs one or more actions when a specific period of time is entered:

   Perform an action on <event>

   If you select an event-based rule, the lower part of the wizard window will display an initial rule description.

   Click the underlined items in the rule description in order to specify its exact content:

- o ***Event***: Clicking the *event* link lets you select the event which must occur in order for the rule to apply (for example *Motion Started*).

- o ***Devices/recording server/management server:*** When you have selected the required event, clicking the *devices/recording server/management server* link lets you specify the devices on which the event should occur in order for the rule to apply. Depending on your event specification, you may be able to select from a list of cameras, inputs, outputs, etc. In this example illustration, the selectable devices are all cameras:

  You specify the required devices by moving them from the *Available devices* list to the *Selected devices* list.

  To move a device from the *Available devices* list to the *Selected devices* list, either select the device and click the *Add* button, double-click the device, or simply drag the device from one list to the other.

  Tip: When devices are grouped into so-called device groups, you can quickly move all devices in a group simply by moving the group folder.

  When the required devices are listed in the *Selected devices* list, click *OK*.

You have now specified the exact content of the first part of the rule description.

Perform an action in a time interval

If you select a time-based rule, no more information is required on the wizard's first step.

4. Click *Next* to go to the wizard's second step. On the wizard's second step you are able to define further conditions for the rule.

5. Select one or more conditions, for example *Day of week is <day>*:

   Depending on your selections, the lower part of the wizard window lets you edit the rule description.

   Click the underlined items in ***bold italics*** to specify their exact content. For example, clicking the *days* link in our example would let you select one or more days of the week on which the rule should apply.

6. Having specified your exact conditions, click *Next* to move to the next step of the wizard and select which actions should be covered by the rule.

   Depending on the content and complexity of your rule, further wizard steps may let you define further information, such as stop events and stop actions. For example, if a rule specifies that a device should perform a particular action during a time interval (for example Thursday between 08.00 and 10.30), the wizard may ask you to specify what should happen when that time interval ends.

7. Your rule is by default active, meaning that once you have created it, it will be applied as soon as the rule's conditions are met.

   If you do not want the rule to be active straight away, clear the *Active* check box.

   Tip: You can always activate/deactivate the rule later.

8. Click *Finish*.

Tip: To view step-by-step descriptions of how to create typically required rules, see Create Typical Rules (on page 116).

Editing, Copying and Renaming a Rule

1. In the Overview pane (see "Panes Overview" on page 36), right-click the required rule.

2. Select either:

   Edit Rule...

   —or—

   Copy Rule...

   —or—

   Rename Rule...

   depending on your needs.

   The wizard *Manage Rule* opens.

3. In the wizard, rename and/or change the rule as required. If you selected *Copy Rule...*, the wizard opens, displaying a copy of the selected rule.

4. Click *Finish*.

Deleting a Rule

Tip: You do not necessarily have to delete an unwanted rule; you may also just temporarily deactivate the rule by clearing the *Active* check box in the *Rule Information* pane for the rule in question, then saving the setting by selecting the Management Client's *File* menu: **Show me where to find the Active check box**

If you wish to delete an existing rule, do the following:

1. In the Overview pane (see "Panes Overview" on page 36), right-click the rule you wish to delete, and select *Delete Rule...*

   Tip: Instead of right-clicking to select *Delete Rule*, you may simply press the DELETE key on your keyboard.

2. You will be asked to confirm that you wish to delete the rule. If you are sure that you wish to delete the rule, click *Yes*.

3. The rule will be removed from the Overview pane's *Rules* list.

Deactivating and Activating a Rule

A rule is by default active, meaning that RC-E will apply the rule as soon as the rule's conditions apply. If you do not want a rule to be active, you can deactivate the rule. When the rule is deactivated, RC-E will not apply the rule, even if the rule's conditions apply. A deactivated rule can easily be activated later.

Deactivating a Rule:

1. In the Overview pane (see "Panes Overview" on page 36), select the required rule.

2. Clear the *Active* check box in the Properties pane (see "Panes Overview" on page 36)

3. Save the setting by clicking *Save* in the Management Client's toolbar (see "Management Client Overview" on page 34).

4. The deactivated rule will be indicated by a different icon in the *Rules* list.

Activating a Rule

When you want to activate the rule again, simply select the required rule, select the *Activate* check box, and save the setting.

Validating Rule(s)

You are able to validate the content of an individual rule or all rules in one step.

Why would I need to validate the content of rules? When you create a rule, the *Manage Rule* ensures that all of the rule's elements make sense. However, when a rule has existed for some time, one or more of the rule's elements may have been affected by other configuration, and the rule may no longer work. For example, if a rule is triggered by a particular time profile, the rule will not work if the time profile in question has subsequently been deleted. Such unintended effects of configuration may be hard to keep an overview of; rule validation helps you keep track of which rules have been affected.

IMPORTANT: Validation takes place on a per-rule basis; each rule is validated in isolation. It is currently not possible to validate rules against each other (for example in order to see whether one rule conflicts with another rule), not even if using the *Validate All Rules* feature.

Furthermore, it is not possible to validate whether configuration of prerequisites outside the rule itself may prevent the rule from working. For example, a rule specifying that recording should take place when motion is detected by a particular camera will validate OK if the elements in the rule itself are correct, even though motion detection (which is enabled on a camera level, not through rules) has not been enabled for the camera in question.

To validate an individual rule or all rules in one step, do the following in the Management Client:

1. In the Overview pane, right-click the rule you wish to validate, and select *Validate Rule* or *Validate All Rules* (depending on your needs):

2. A simple dialog will inform you whether the rule(s) validated successfully or not. If you chose to validated more than one rule and one or more rules did not succeed, the dialog will list the names of the affected rules.

Manage Time Profiles

Time profiles are periods of time defined by the administrator. Time profiles can be used when creating rules (see "Manage Rules" on page 133), for example, a rule specifying that a certain action should take place within a certain time period. An alternative to Time profiles are Day Length Time profiles (see "Manage Day Length Time Profiles" on page 140).

Time profiles are assigned to roles (see "Manage Roles" on page 147). By default, all roles are assigned the default time profile *Always.* This means that members of roles with this default time profile attached has no time-based limits to their user rights in the RC-E system. An alternative time profile can easily be assigned to a role.

Time profiles are highly flexible: they can be based on one or more single periods of time, on one or more recurring periods of time, or a combination of single and recurring times. Many users will be familiar with the concepts of single and recurring time periods from calendar applications, such as the one in Microsoft Outlook.

Time profiles always apply in local time. This means that if your system has recording servers placed in different time zones, any actions (e.g. recording on cameras) associated with time profiles will be carried out in each recording server's local time. Example: If you have a time profile covering the period 08.30 to 09.30, any associated actions on a recording server placed in New York will be carried out when the local time is 08.30 to 09.30 in New York, while the same actions on a recording server placed in Los Angeles will be carried out some hours later, when the local time is 08.30 to 09.30 in Los Angeles.

Time profiles are created and managed in the Management Client by expanding the Site Navigation pane (see "Panes Overview" on page 36)'s *Rules and Events* folder, then selecting *Time Profiles*. A *Time Profiles* list will appear in the overview pane.

Specifying a Time Profile

1. In the *Time Profiles* list, right-click *Time Profiles*, and select *Add Time Profile...*:

   Tip: Instead of right-clicking to select *Add Time Profile...*, you can press CTRL+N on your keyboard.

   This will open the *Time Profile* window.

2. In the *Time Profile* window, type a name for the new time profile in the *Name* field. Optionally, type a description of the new time profile in the *Description* field.

3. In the *Time Profile* window's calendar, select either *Day View, Week View* or *Month View*, then right-click inside the calendar and select either *Add Single Time*... or *Add Recurrence Time...*

   Tip: If you select a time period by dragging in the calendar before right-clicking, the selected period will automatically be used in the dialog that appears when you select *Add Single Time...* or *Add Recurring Time...*

   Specifying a Single Time

   When you select *Add Single Time...*, the *Select Time* window appears:

1. In the *Select Time* window, specify *Start time* and *End time*. If the time is to cover whole days, select the *All day event* box.

2. Click *OK*.

Tip: A time profile is able to contain several periods of time. If you want your time profile to contain further periods of time, add more single times or recurring times.

   Specifying a Recurring Time

   When you select *Add Recurring Time...*, the *Select Recurring Time* window appears:

1. In the *Select Time* window, specify time range, recurrence pattern and range of recurrence.

2. Click *OK*.

Tip: A time profile is able to contain several periods of time. If you want your time profile to contain further periods of time, add more single times or recurring times.

1. When you have specified the required time periods for your time profile, click *OK* in the *Time Profile* window. Your new time profile is added to the *Time Profiles* list in the Overview pane (see "Panes Overview" on page 36).

   If at a later stage you wish to edit or delete the time profile, you can do that from the *Time Profiles* list.

Editing a Time Profile

1. In the Overview pane (see "Panes Overview" on page 36)'s *Time Profiles* list, right-click the required time profile, and select *Edit Time Profile...*

   Tip: Instead of right-clicking to select *Edit Time Profile*, you can select the required time profile and press F2 on your keyboard.

   This will open the *Time Profile* window.

2. In the *Time Profile* window, edit the time profile as required.

   When you have made the required changes to the time profile, click *OK* in the *Time Profile* window. You will be returned to the Overview pane's *Time Profiles* list.

Tip: In the *Time Profile Information* window, edit the time profile as required. Remember that a time profile may contain more than one time period, and that time periods may be recurring.

Tip: The small month overview in the top right corner of the *Time Profile Information* window can help you get a quick overview of the time periods covered by the time profile, as dates containing specified times are highlighted in bold. In this example, the bold dates indicate that time periods have been specified on several days, and that a recurring time may have been specified on Mondays.

Manage Day Length Time Profiles

When cameras are placed outside, it is often required to lower the cameras resolution, enable black/white, or change other settings when it gets dark or vice versa when it gets light. The further north or south from the equator the cameras are placed, the more the sunrise and sunset time varies during the year. This makes it impossible to use normal fixed time profiles (see "Manage Time Profiles" on page 138) to adjusts camera settings according to light conditions.

To overcome this, Day Length Time profiles can be created and defined in RC-E according to the sunrise and sunset in a specified geographical area. Via GPS coordinates, the system, on a daily basis, calculates the sunrise and sunset time, even incorporating daylight saving time. As a result, it automatically follows the yearly changes in sunrise/sunset in the selected area, ensuring the profile to be active only when needed. All times and dates are based on the management servers time and date settings.

In addition, it is possible to set a positive or negative offset (in minutes) for the start (sunrise) and end time (sunset). The offset for the start and the end time can be identical or different.

Day Length Time profiles can be used when creating both rules (see "Manage Rules" on page 133) and roles (see "About Roles" on page 145).

Creating a Day Length Time Profile

1. In the Management Client, expanding the Site Navigation pane (see "Panes Overview" on page 36)'s *Rules and Events* folder, select *Time Profiles*.
2. In the overview pane, in the *Time Profiles* list, right-click *Time Profiles*, and select *Add Day Length Time Profile....*
3. In the *Day Length Time Profile* window, fill in the needed information. In order to deal with transition periods between lightness and darkness, it is possible to offset activation and deactivation of the profile.

   Furthermore, time and month names are shown in the language dictated by your computer's language/regional settings.
4. To see the location of the entered GPS coordinates in a map, click *Show Position in Browser...* (will open a browser).
5. Click *OK*.

Day Length Time Profile Properties

- ***Name:*** Name of the profile.
- ***Description*** (optional): Description of the profile.
- ***GPS coordinates:*** GPS coordinates indicating the physical location of the camera(s) assigned to the profile.
- ***Sunrise offset:*** Number of minutes (+/-) by which activation of the profile is offset by sunrise.
- ***Sunset offset:*** Number of minutes (+/-) by which deactivation of the profile is offset by sunset.

- ***Time zone:*** Time zone indicating the physical location of the camera(s).

Manage Notification Profiles

With notification profiles you can set up ready-made e-mail notifications, which can automatically be triggered by a rule (see "Manage Rules" on page 133), for example when a particular event occurs. You are even able to include still images and AVI video clips in the e-mail notifications.

Note that when using the SMTP Service with .NET 4.0, it is not possible to send attachments over 3 MB. However two hotfixes (must be installed on the management server in the listed order) from Microsoft can be found at:
http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226 (see http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226 - http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226)
http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723 (see http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723 - http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723)

TLS (Transport Layer Security) and its predecessor SSL (Secure Socket Layer) is not supported; if the sender belongs on a server that requires TLS or SSL, e-mail notifications will not work properly. Also, you may be required to disable any e-mail scanners that could prevent the application sending the e-mail notifications.

Prerequisites

Before you can create notification profiles, you must specify settings for the outgoing SMTP mail server you are going to use for the e-mail notifications.

Optionally, if you want the notification profile's e-mail notifications to be able to contain AVI video clips, the compression settings for use when generating the AVI files must also be specified.

1. Go to the Management Client's menu bar, and select *Tools > Options...* This will open the *Options* window.
   - For **outgoing SMTP Mail Server**: Specify settings for the outgoing SMTP mail server on the *Mail Server* tab. For more information, see Outgoing SMTP Mail Server Settings (on page 171).
   - For **AVI Compression**: Specify compression settings the *AVI Generation* tab. For more information, see AVI Compression Settings (on page 170).

Adding New Notification Profiles

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Rules and Events*, right-click *Notification Profiles*, and select *Add Notification Profile...* This will open the *Add Notification Profile* wizard.
2. On the wizard's first step, specify name and description.

   Click *Next*.
3. On the wizard's second step, verify that *Email* is selected, click *Next*.
4. On the wizard's third step, specify recipient, subject, message text and time between e-mails.
5. If you want send a test e-mail notification to the specified recipients, click *Test E-mail*.
6. If you want to include pre-alarm still images in e-mail notifications under the notification profile, select *Include images*, and specify number of images, time between images and whether images should be embedded in e-mail or not.

7. If you want to include AVI video clips in e-mail notifications under the notification profile, select *Include images*, and specify time before and after event and frame rate.

8. Click *Finish*.

IMPORTANT: Pre-alarm images functionality cannot coexist with edge recording, see Enabling and Disabling Edge Recording—Camera Only (on page 106). So if a camera is setup to export pre-alarm images it is not possible to enable edge recording on that camera, and vice versa.

Using Rules to Trigger E-mail Notifications

You use the *Manage Rule* for creating rules. The wizard takes you through all required steps. You specify the use of a notification profile during the step on which you specify the rule's actions.

When selecting the action *Send notification to <profile>*, you get the option of selecting the required notification profile. You also get the option of selecting which cameras any recordings to be included in the notification profile's e-mail notifications should come from:

Keep in mind that recordings cannot be included in the notification profile's e-mail notifications unless something is actually being recorded.

If still images or AVI video clips are required in the notification profile's e-mail notifications, you should therefore verify that the rule you are creating— or another existing rule— specifies that recording should take place

For more information about rules in general, see Manage Rules (on page 133).

Fill in Notification Profile Details

- ***Name*:** (Compulsory) Type a descriptive name for the notification profile. The name will later appear whenever you select the notification profile during the process of creating a rule.

- ***Description*:** (Optional) Type a description of the notification profile. The description will, among other places, appear when you pause your mouse pointer over the notification profile in the Overview pane's *Notification Profiles* list:

- ***Recipients*:** Type the e-mail addresses to which the notification profile's e-mail notifications should be sent.

  If typing more than one e-mail address, separate addresses with a semicolon. Example: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc

  ***Subject* :** Type the text you want to appear as the subject of the e-mail notifications.

  Tip: You can insert system variables, such as *Device name*, in the subject and message text field. To insert variables, click the required variable links in the box below the field.

- ***Message text:*** Type the text you want to appear in the body of the e-mail notifications. In addition to the message text, the body of each e-mail notification will automatically contain this information:

  - What triggered the e-mail notification.

  - The source of any attached still images or AVI video clips

- ***Time btw. e-mail:*** Specify required minimum time (in seconds) to pass between the sending of each e-mail notification. Examples:

  - If specifying a value of *120*, a minimum of 2 minutes will pass between the sending of each e-mail notification, even if the notification profile is triggered again by a rule before the 2 minutes have passed.

    If specifying a value of *0*, e-mail notifications will be sent each time the notification profile is triggered by a rule. This can potentially result in a very large number of e-mail notifications being sent. If using the value

0, you should therefore carefully consider whether you want to use the notification profile in rules which are likely to be triggered frequently.

- ***Number of images:*** Specify the maximum number of still images you want to include in each of the notification profile's e-mail notifications. Default is five images.
- ***Time btw. images (ms)*****:** Specify the number of milliseconds you want between the recordings presented on the included images. Example: With the default value of 500 milliseconds, the included images will show recordings with half a second between them.
- ***Embed images in e-mail:*** If selected (default), images will be inserted in the body of e-mail notifications. If not, images will be included in e-mail notifications as attached files. **Example**

  Example of e-mail notification with embedded images. Note that the size of the embedded images will depend on individual camera settings.
- ***Time before event (secs.):*** This setting is used to specify the start of the AVI file. By default the AVI file will contain recordings from 2 seconds before the notification profile is triggered; you are able to change this to the number of seconds you require.
- ***Time after event (secs.):*** This setting is used to specify the end of the AVI file. By default the AVI file will end 4 seconds after the notification profile is triggered; you are able to change this to the number of seconds you require.
- ***Frame rate:*** Specify the number of frames per second you want the AVI file to contain. Default is five frames per second. The higher the frame rate, the higher the image quality and AVI file size.

Manage User-defined Events

User-defined events are events which are custom made to suit your system. Like other events, user-defined events can be used in rules (see "Manage Rules" on page 133) in order to trigger actions. Thus, when a user-defined event occurs, a rule can trigger that one or more actions should take place on the RC-E system.

Example: When user-defined event 37 occurs, PTZ camera 224 should stop patrolling and go to preset position 18.

Through roles (see "Manage Roles" on page 147), you define which of your users should be able to trigger the user-defined events; see Specify Rights of a Role (on page 150) for more information.

User-defined events can be used in two ways, simultaneously if required:

- **For Providing the Ability to Manually Trigger Events in the Ocularis Client**

  In this case, user-defined events make it possible for end users to manually trigger events while viewing live video in the Ocularis Client. Thus, when a user-defined event occurs because it is manually triggered by an Ocularis Client user, a rule can trigger that one or more actions should take place on the OnSSI RC-E system.
- **For Providing the Ability to Trigger Events through API**

  In this case, user-defined events can be triggered from outside the surveillance system. Using user-defined events this way requires that a separate API (Application Program Interface; a set of building blocks for creating or customizing software applications) is used when triggering the user-defined event. Authentication through Active Directory is required for using user-defined events this way. This ensures that even though the user-defined events can be triggered from outside the surveillance system, only authorized users will be able to do it.

  Also, user-defined events can via API be associated with meta-data, defining certain devices or device groups. This is highly usable when using user-defined events to trigger rules: you avoid having a rule for each

device, basically doing the same thing. Example: A company uses access control, having 35 entrances, each with an access control device. When an access control device is activated, a user-defined event is triggered in RC-E. This user-defined event is used in a rule to start recording on a camera associated with the activated access control device. It is defined in the meta-data which camera is associated with what rule. This way the company does not need to have 35 user-defined events and 35 rules triggered by the user-defined events; a single user-defined event and a single rule are enough.

Whichever way you choose to use user-defined events, each user-defined event must first be added through the Management Client:

Adding a New User-defined Event

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Rules and Events*, and select *User-defined Events*.
2. In the Overview pane (see "Panes Overview" on page 36), right click *Events* and select *Add User-defined Event...*
3. Type a name for the new user-defined event, and click *OK*. The newly added user-defined event will now appear in the list in the Overview pane.

   User rights permitting (see roles (see "About Roles" on page 145)), the user-defined event can now be manually triggered from Ocularis Clients. Already connected Ocularis Client users must log out and log in again before the user-defined event will be visible.

   Remember to create one or more rules (see "Manage Rules" on page 133) specifying what should take place when the custom event occurs.

Editing the Name of an Existing User-defined Event

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Rules and Events*, and select *User-defined Events*.
2. In the Overview pane (see "Panes Overview" on page 36), select the required user-defined event.
3. In the Properties pane (see "Panes Overview" on page 36), overwrite the existing name.
4. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

   Already connected Ocularis Client users must log out and log in again before the name change will be visible.

Deleting an Existing User-defined Event

Keep in mind that deleting a user-defined event will affect any rules in which the user-defined event is used.

A deleted user-defined event will not disappear from Ocularis Clients immediately; only after Ocularis Client users log out.

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Rules and Events*, and select *User-defined Events*.
2. In the Overview pane (see "Panes Overview" on page 36), right click the unwanted user-defined event, and select *Delete New User-defined Event...*
3. You will be asked to confirm that you want to delete the user-defined event; if you are sure, click *Yes*.

Security

About Security

In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), you are able to work with the following under *Security*:

- ***Roles* :** (see "About Roles" on page 145) Roles determine which of your RC-E solution's features users and groups (see "Manage Users and Groups" on page 145) are able to use. In other words, roles determine rights.

About Roles

Roles determine which of your RC-E solution's features users and groups (see "Manage Users and Groups" on page 145) are able to use. In other words, roles determine rights and handles security within the application.

You define roles first, then you add users/groups and a time profile (see "Manage Time Profiles" on page 138) to each role.

One role is predefined in RC-E , and cannot be deleted: the *Administrators* role. In addition to the *Administrators* role, you are able to add as many roles as required in your organization.

To manage roles in RC-E , expand the *Security* folder in the Management Client's Site Navigation pane (see "Panes Overview" on page 36), and select *Roles*.

For more information see:

- Manage Users and Groups (on page 145)
- Assign and Remove Users and Groups to/from Roles (on page 149)
- Manage Roles (on page 147)
- Specify Rights of a Role (on page 150).

Note that roles may also determine access to views in clients; see Manage View Groups (on page 108).

Manage Users and Groups

In RC-E , you define roles (see "About Roles" on page 145) first, then you add users/groups to the roles.

Roles determine which of RC-E's features users and groups are able to use. In other words, roles determine rights.

Once you have defined roles, you can add users and groups; see Assign and Remove Users & Groups to/from a Role (see "Assign and Remove Users and Groups to/from Roles" on page 149).

Prerequisites

In order to be able to add users and groups through the Active Directory service, a server with Active Directory installed, and acting as domain controller, must be available on your network. Consult your network administrator if in doubt.

Adding Users and Groups through Active Directory (Normal Way)

Users and groups are normally added from Active Directory, although users can also be added without Active Directory.

What is Active Directory? Active Directory is a distributed directory service included with several Windows Server operating systems; it identifies resources on a network in order for users or applications to access them. Users as well as groups are specified centrally in Active Directory.

Using Active Directory for adding existing user and group information to RC-E has several benefits: The fact that users as well as groups are specified centrally in Active Directory means that you will not have to create any user accounts from scratch in RC-E. It also means that you will not have to configure any authentication of users on RC-E; authentication is handled by Active Directory.

Active Directory User and Group Concepts

Active Directory uses the concepts of users and groups.

Users

Users are Active Directory objects representing individuals with a user account.

Groups

Groups are Active Directory objects capable of containing several users. In this example, the Management Group has three members (i.e. it contains three users).

Groups can contain any number of users. By adding a group to RC-E, you add all of its members in one step. Once the group has been added to RC-E, any changes subsequently made to the group in Active Directory (such as new members added or old members removed) will immediately be reflected in RC-E.

Note that a user can be a member of more than one group at a time.

Adding Users Not Using Active Directory

While you primarily add RC-E users and groups to roles (see "About Roles" on page 145) through Active Directory, it is also possible to add individual users—but not groups—without Active Directory. If not using Active Directory, note the following:

- When installing the management server, the user under which the management server service runs must be a local PC user on the server. See also Management Server Installation (see "Install Management Server" on page 13).
- On the computer running the management server, simple file sharing must be disabled the following way:
    1. On the computer running management server, right-click *Start*, and select *Explore*.
    2. In the window that opens, select the *Tools* menu, then select *Folder Options...*
    3. Select the *View* tab.
    4. Scroll to the bottom of the *Advanced settings* list, and make sure that the *Use simple file sharing (Recommended)* check box is cleared.
    5. Click OK, and close the window.
- You add users to roles through the Management Client almost as when adding users from Active Directory (see Assign and Remove Users & Groups to/from a Role (see "Assign and Remove Users and Groups to/from Roles" on page 149). However, when adding users, you must refer to particular users on particular computers, as in this example where the user USER001 on the computer PC001 is added.

  When users added this way log in to RC-E, the user must *not* specify any server name, PC name, or IP address as part of their user names. Example of a correctly specified user name: USER001. Example of an incorrectly specified user name: PC001/USER001. The users should of course still specify their passwords, etc.

Manage Roles

Roles determine which of your RC-E solution's features users and groups (see "Manage Users and Groups" on page 145) are able to use. In other words, roles determine rights and handles security within the application.

You define roles first, then you add users/groups and a time profile to each role. Added roles automatically also become view groups (see "Manage View Groups" on page 108). These are only used with Ocularis Client Limited Mode.

One role is predefined in RC-E , and cannot be deleted: the *Administrators* Role.

In addition to the *Administrators* role, you are able to add as many roles as required in your organization.

To manage roles in RC-E , expand the *Security* folder in the Management Client's Site Navigation pane (see "Panes Overview" on page 36), and select *Roles*.

For more information see also Assign and Remove Users and Groups to/from Roles **(on page 149) and** Specify Rights of a Role **(on page 150).**

Note that roles may also determine access to views in clients; see Manage View Groups (on page 108).

More About Administrators role

The *Administrators* role is predefined, and cannot be deleted. Users and groups with the *Administrators* role have complete and unrestricted access to the entire RC-E system. For this reason it is not necessary to specify role settings for the *Administrators* role. Because the *Administrators* role has complete and unrestricted access, it does not have a time profile (see "Manage Time Profiles" on page 138).

You add users and groups to the *Administrators* role just as with any other role; see Assign and Remove Users and Groups to/from Roles (on page 149).

IMPORTANT: Users with *local machine administrator* rights on the computer running the management server will automatically have administrator rights on the management server. It is therefore important that you verify which users have *local machine administrator* rights on the computer running the management server: Only users whom you trust as administrators of your RC-E system should have *local machine administrator* rights on the computer running the management server.

Adding a Role and Manage its Time Profiles

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Security*, and right-click *Roles*.
2. Select *Add Role*. This will open the *Add Role* dialog.
3. In the *Add Role* dialog, type a name and description of the new role.
4. Then click *OK*.
5. The new role is added to the *Roles* list in the Overview pane (see "Panes Overview" on page 36). By default, a new role does not have any users/groups associated with it, but it does have the default time profile *Always* associated.
6. To change the default time profile, in the Properties pane (see "Panes Overview" on page 36), click the desired drop down dialog.
7. You are now able to assign users/groups to the role, and to specify which of RC-E's features they should be able to access. See Assign and Remove Users & Groups to/from a Role (see "Assign and Remove Users and Groups to/from Roles" on page 149) and Specify Rights of a Role (on page 150).

Copying a Role

If you have a role with complicated settings and/or rights and need a similar—or almost similar—role, it might be easier to copy the already existing role and make minor adjustments to the copy than to creating a new role from scratch.

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Security*, click *Roles,* right-click the required role in the Overview pane (see "Panes Overview" on page 36), select *Copy Role...*
2. In the dialog that opens, give the copied role a new unique name and description.
3. Click *OK*.

Deleting a Role

Before deleting a role (see "About Roles" on page 145), keep in mind that you are able to delete a role even when users and/or groups have been assigned to the role. It is therefore often a good idea to verify if any users/groups are assigned to the role before deleting it.

Verifying if Any Users/Groups Are Assigned to a Role

- In the Management Client's Site Navigation pane, expand *Security*, and right-click *Roles*.
- Select the required role in the Overview pane (see "Panes Overview" on page 36), then select the *Users and Groups* tab in the Properties pane. Any users and/or groups assigned to the role will be listed on the *Users and Groups* tab.

How to Delete a Role

Deleting a role will not delete a view group based upon the role. For information about deleting view groups, see Manage View Groups (on page 108).

1. In the Management Client's Site Navigation pane, expand *Security*, and right-click *Roles*.
2. Right-click the unwanted role in the Overview pane, and select *Delete Role*.

   Tip: Alternatively, press DELETE on your keyboard.
3. Click *Yes*.

Renaming a Role

Renaming a role will not change the name of a view group based upon the role. For information about renaming view groups, see Manage View Groups (on page 108).

1. In the Management Client's Site Navigation pane, expand *Security*, and right-click *Roles*.
2. Right-click required role in the Overview pane (see "Panes Overview" on page 36), and select *Rename Role...*

   Tip: Alternatively, press F2 on your keyboard.
3. In the dialog that opens, change the name of the role.

   Tip: You are also able to change the description of the role.

4. Click *OK*.

Viewing Effective Roles

With the Effective Roles feature, you are able to view all roles (see "About Roles" on page 145) of a selected user or group (see "Manage Users and Groups" on page 145). This ability is especially convenient if you are using groups; in fact it is the only way of viewing the roles of individual group members.

1. Open the *Effective Roles* window. There are three ways in which you can open the *Effective Roles* window:
   - From the Management Client's menu bar, by selecting *Tools* > *Effective Roles...*
   - From the Overview pane (see "Panes Overview" on page 36) (when working with roles), by right-clicking anywhere inside the pane, then selecting *Effective Roles*...
   - From the Site Navigation pane, by expanding *Security*, then right-clicking *Roles*, then selecting *Effective Roles*...
2. In the *Effective Roles* window's *User name* field, type the user name of the required user.

   Tip: By clicking the browse button to the right of the field, you are able to browse for the user in question, using Active Directory.
3. If you typed the user name directly into the *User name*, click *Refresh* in the lower part of the window to display the roles of the user.

   If you used Active Directory to browse for the user, the user's roles will be displayed automatically.

Assign and Remove Users and Groups to/from Roles

To assign or remove users or groups to/from a role, do the following:

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Security*, and select *Roles*. Then select the required role in the overview pane (see "Panes Overview" on page 36).
2. In the properties pane (see "Panes Overview" on page 36), select the *Users & Groups* tab.

Assigning Users and Groups to a Role

a On the *Users & Groups* tab, click *Add...*. This will open the *Select Users, Computers or Groups* dialog.

b Verify that the required object type is specified. If, for example, you need to add a computer, click *Object Types* and mark *Computer*. Furthermore, verify that the required domain is specified in the *From this location* field. If not, click *Locations...* to browse for the required domain.

c In the *Enter the object names to select* box, type the required user names, initials, or other types of identifier which Active Directory will be able to recognize.

Tip: Typing part of a name is often enough. Use the Check Names feature to verify that the names, initials, etc. you have typed are recognized by Active Directory.

d Click *OK*. The selected users/groups are now added to the *Users & Groups* tab's list of users who have been assigned the selected role:

Removing Users and Groups from a Role

Tip: To find out which roles user, groups, or individual group members have, use the Effective Roles (see "Manage Roles" on page 147) feature.

Keep in mind that a user may also have roles through group memberships. When that is the case, you cannot remove the individual user from the role. Furthermore group members may also hold roles as individuals.

a On the *Users & Groups* tab, select the user or group you want to remove, then click *Remove* in the lower part of the tab.

Tip: You can select more than one user or group, or a combination of groups and individual users, if required.

b Confirm that you want to remove the selected user(s) or and group(s). Click *Yes*.

Specify Rights of a Role

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Security*, and select *Roles*. Then select the required role in the overview pane (see "Panes Overview" on page 36).

2. In the properties pane (see "Panes Overview" on page 36), specify required rights for the role on the relevant tabs:

Device Rights

The *Device* tab lets you specify which features users/groups with the selected role should be able to use for each device (e.g. a camera) or device group.

The tab is divided into two halves: In the upper half you select the device or device group for which you want to specify role rights. In the lower half you then specify which of the selected device's or device group's features users/groups with the selected role should have the right to access.

Remember to repeat for each required device/device group.

Camera-Related Rights

Setting determines whether...

- ***AUX Commands:***...it will be possible to use auxiliary commands from the Ocularis Client.

  What are AUX Commands? AUX is short for Auxiliary. Such commands offer the user control of, for example, wipers on a camera connected via a video server. Camera-associated devices connected via auxiliary connections are controlled from the Ocularis Client.

- ***Add****:* ...it will be possible to add bookmarks in recorded video from the Ocularis Client.

- ***Delete****:* ...it will be possible to delete bookmarks in recorded video from the Ocularis Client.

- ***Edit****:* ...it will be possible to edit bookmarks in recorded video from the Ocularis Client.

- ***View****:*...it will be possible to view bookmarks in recorded video from the Ocularis Client.

- ***View live within time profile*:** ...live viewing of video from the selected camera(s) will be possible in access clients.

- ***Export video:*** ..the database export feature can be used when browsing recorded video from selected camera(s) in the Ocularis Client. Furthermore, the AVI, JPEG and export features can be used in similar way in all access clients.

- ***Get sequences:*** ...the *Sequences* feature can be used when browsing recorded video from the selected camera(s) in access clients.
- ***Playback Video:***...playing back of recorded video from the selected camera(s) will be possible in access clients.
- ***Smart Search:*** ...the *Smart Search* feature can be used when browsing recorded video from the selected camera(s) in the Ocularis Client.
- ***Visible****:* ...the selected camera(s) will be visible in access clients.

The *View live* right also requires that the role has been granted the right to view the access clients' *Live* tab. This right is granted as part of the application rights.

The *Export Video* and *Playback Video* rights also require that the role has been granted the right to view the access clients' *Browse* tab. This right is granted as part of the application rights.

Microphone-Related Rights

Setting determines whether...

- ***Visible*****:** ...the selected microphone(s) will be visible in the Ocularis Client.
- ***Listen to live audio:***...listening to live audio from the selected microphone(s) will be possible in the Ocularis Client.
- ***Browse audio:*** ...browsing of recorded audio from the selected microphone(s) will be possible in the Ocularis Client.
- ***Export audio*****:** ...the export feature can be used when browsing recorded audio from the selected microphone(s) in the Ocularis Client.
- ***Get sequences:*** **This feature is currently not supported** ...the *Sequences* feature can be used when browsing recorded audio from the selected microphone(s) in the Ocularis Client.

Speaker-Related Rights

Setting determines whether...

- ***Visible*****:** ...the selected speaker(s) will be visible in the Ocularis Client.
- ***Listen to live audio:***...listening to live audio from the selected speaker(s) will be possible in the Ocularis Client.
- ***Browse audio:*** ...browsing of recorded audio from the selected speaker(s) will be possible in the Ocularis Client.
- ***Export audio:***...the export feature can be used when browsing recorded audio from the selected speaker(s) in the Ocularis Client.
- ***Get sequences*****: This feature is currently not supported** ...the *Sequences* feature can be used when browsing recorded audio from the selected speaker(s) in the Ocularis Client.

IMPORTANT: Although what is being said through a speaker can be recorded and archived (see "About Storage and Archiving" on page 56), there is currently no way of playing back or exporting such recorded outgoing audio. Therefore, some of the speaker-related rights currently have no effect. Features for playing back and exporting recorded outgoing audio, etc. will be available in subsequent releases as soon as possible.

Input-Related Rights

- ***Visible*:** Determines whether information about the selected input(s) will be visible to users of the Ocularis Client , an add-on product for providing complete overview of surveillance system status and alarms.

Output-Related Rights

Setting determines whether...

- ***Visible*:** ...the selected output(s) will be visible in the Ocularis Client. If visible, the output will be selectable on a list in the Ocularis Client.
- ***Activate output:*** ...the selected output(s) can be activated from the Ocularis Client.

Outputs are selected and activated on the Ocularis Client's *Live* tab. Both rights thus require that the role has been granted the right to view the Ocularis Client's *Live* tab; this right is granted as part of the application security rights.

PTZ Rights

Relevant only if PTZ (Pan/Tilt/Zoom) cameras are available on your RC-E system, the *PTZ* tab lets you specify which features users/groups with the selected role should be able to use.

The *PTZ* tab is divided into two halves: In the upper half you select the PTZ camera or device group for which you want to specify settings— note that only PTZ cameras and device groups containing PTZ cameras are available for selection. In the lower half you then specify what users/groups with the selected role should be able to do when operating the selected PTZ cameras.

Setting determines whether users/groups...

- ***Allow PTZ Control:***...with the selected role are able to use the pan, tilt and zoom features of the selected PTZ camera(s).
  - False: Users/groups with the selected role will not be able to use the pan, tilt and zoom features of the selected PTZ camera(s)
  - True: Users/groups with the selected role will be able to use the pan, tilt and zoom features of the selected PTZ camera(s)
- ***PTZ Priority:***...have priority for PTZ cameras and how. When several users on a surveillance system wish to control the same PTZ camera at the same time, conflicts may occur. This setting lets you alleviate the problem by specifying a priority for use of the selected PTZ camera(s) by users/groups with the selected role. Specify a priority from*1*to*32.000*, where*1*is the lowest priority.

  Default PTZ priority is 3000.

  Example: You specify that the role *Security Manager* should have very high priority when using a PTZ camera, whereas the role *Security Assistant* should have low priority when using the PTZ camera. Now, if a user with the role *Security Manager* and a user with the role *Security Assistant* want to control the PTZ camera at the same time, the user with the role *Security Manager* will win the ability to control the camera.

  If your system is upgraded from an older version of RC-E, the old values (*Very Low, Low, Medium, High* and *Very High*) have been translated as follows:
  - *Very Low = 1000*
  - *Low = 2000*
  - *Medium = 3000*

- *High = 4000*
- *Very High = 5000*

- ***Allow activation of PTZ presets:*** ...with the selected role are able to move the selected PTZ camera(s) to preset positions.
  - False: Users/groups with the selected role will not be able to move the selected PTZ camera(s) to preset positions
  - True: Users/groups with the selected role will be able to move the selected PTZ camera(s) to preset positions

Speech Rights

Relevant only if loudspeakers are available on your RC-E system.

The *Speech* tab is divided into two halves: In the upper half you select the speaker or device group for which you want to specify settings. In the lower half you then specify what users/groups with the selected role should be able to do when operating the selected speaker(s).

The following rights are available:

- ***Speak live:*** Determines whether users with the selected role will be able talk through the selected speaker(s).
- ***Speak priority:*** When several Ocularis Client users want to talk through the same speaker at the same time, conflicts may occur. This setting lets you alleviate the problem by specifying a priority for use of the selected speaker(s) by users/groups with the selected role. Specify a priority from *Very low* to *Very high*.

  Example: You specify that the role *Security Manager* should have very high priority when talking through a speaker, whereas the role *Security Assistant* should have low priority when talking through the speaker. Now, if a user with the role *Security Manager* and a user with the role *Security Assistant* want to talk through the speaker at the same time, the user with the role *Security Manager* will win the ability to talk.

If two users with the same role want to speak at the same time, the first-come first-served principle applies.

Application Rights

The *Application* tab lets you specify which applications in your RC-E system users/groups with the selected role should be able to use. Users must be a member of the *Administrator* role to have access to the Management Client. Simply select the required applications:

Setting determines whether users/groups with the selected role are able to use the...

- ***Browse***: ...*Browse* tab in the Ocularis Client (when used in Limited Mode).
- ***Live*****:** ...*Live* tab in the Ocularis Client (when used in Limited Mode).
- ***Setup*****:** ...*Setup* button in the Ocularis Client (when used in Limited Mode).

External Event Rights

The *External Events* tab is divided into two halves. In the upper half, select the external event for which you want to specify settings. In the lower half, specify what users/groups with the selected role should be able to do with the selected external event in the Ocularis Client.

- ***Trigger external event with time profile:*** In the Ocularis Client's *Live* mode it is possible to manually trigger your surveillance system's external events.

View Group Rights

The *View Group* tab lets you specify which view groups (i.e. groups of views in clients; see Manage View Groups (on page 108) for more information) users/groups with the selected role should be able to use.

The tab is divided into two halves: In the upper half you select the view group for which you want to specify role rights. In the lower half you then specify how users/groups with the selected role should be able to access the selected view group.

Setting determines whether users/groups with the selected role are able to work when using Ocularis Client in Limited Mode.

Server Rights

Specifying role rights on the *Servers* tab is only relevant if you have integrated NetDVMS or RC-C servers into your RC-E solution; see Manage RC-C Servers (on page 162) for more information.

The tab is divided into two halves: In the upper half you select the server for which you want to specify role rights. In the lower half you then specify which authentication settings should apply for users/groups with the selected role. The process is described in detail in Defining Access Roles for OnSSI RC-C Servers (see "Manage RC-C Servers" on page 162).

NetMatrix Rights

Specifying role rights on the *NetMatrix* tab is only relevant if you have configured NetMatrix recipients on your RC-E system.

From the Ocularis Client it is possible to send video to selected NetMatrix recipients. The *NetMatrix* tab lets you specify which NetMatrix recipients should be selectable for this purpose in the Ocularis Client.

The tab is divided into two halves: In the upper half you select the NetMatrix recipient for which you want to specify role rights. In the lower half you then specify if users/groups with the selected role should be able to select the NetMatrix recipient in the Ocularis Client when used in Limited Mode.

Manage View Groups

The way in which video from one or more cameras is presented in clients is called a view. A view group is basically a container for one or more logical groups of such views.

View Groups configured in RC-E will only be accessible via Ocularis Client in Limited Mode. Standard views are configured on the Ocularis Base using the Ocularis Administrator application.

More about View Groups

By default, each role you define in the Management Client is also created as a view group: when you add a role in RC-E Manager, the role will by default appear as a view group for use in Ocularis Client Limited Mode.

- A view group based on a role will by default only be available to users/groups who have been assigned to the role in question. You are able to change this; see *View Group Rights* in Specify Rights of a Role (on page 150).

- A view group based on a role will by default carry the role's name.

  Example: If you create a role with the name *Building A Security Staff*, it will by default appear in Ocularis Client Limited Mode as a view group called *Building A Security Staff*. You are able to change the name; see the following for more information.

- In addition to the view groups that are created when roles are added, you are able to create as many other view groups as you require. You can also delete view groups which you do not want to use, including those automatically created when adding roles.
- Even though a view group is created each time you add a role (see "Manage Roles" on page 147), view groups do not have to correspond to roles. You are therefore able to add any number of view groups—if required—and rename or remove each of your view groups if required. This is no matter whether the view groups were created automatically when adding a role or whether you added them manually.

Adding a View Group

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand the Clients node, right-click View Groups, and select *Add View Group*. This opens the *Add View Group* dialog.
2. Type the name of the new view group, then click *OK*.
3. Optionally; in the Management Client's overview pane, select the added view group, then in the properties pane add a description of the view group.

No roles will have the right to use the newly added view group until you have specified such rights; see *View Group Rights* in Specifying the Rights of a Role (see "Specify Rights of a Role" on page 150) for more information.

Also, even when you have specified which roles should be able to use the newly added view group, already connected client users with the relevant roles must log out and log in again before they will be able to see the view group.

Renaming a View Group

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand Clients, and select *View Groups*.
2. In the Management Client's overview pane, right-click the required view group and select *Rename View Group*.
3. Change the view group's name as required, then press the return key on your keyboard.

Client users already connected must log out and log in again before the name change will be visible.

Removing a View Group

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand Clients and select *View Groups*.
2. In the Management Client's overview pane, right-click the required view group and select *Delete View Group*.
3. Click *Yes*.

System Dashboard

About System Dashboard

In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), you are able to work with the following under *System Dashboard*:

- ***System Monitor:*** (see "About System Monitor" on page 156)Here you can view and print detailed system reports on servers, devices and cameras.
- ***Current Task:*** (see "About Current Task" on page 157)Here you can get an overview of tasks under a selected recording server.
- ***Configuration Report:*** (see "About Configuration Report" on page 157) From here you can decide what to include in, and print, RC-E system configuration reports.

About System Monitor

From the Site Navigation pane (see "Panes Overview" on page 36), expand *System Dashboard*, and click *System Monitor*. This brings up the system monitor using embedded browser technology.

If you access the system monitor from a **server** operating system, you might experience a message regarding *Internet Explorer Enhanced Security Configuration*. Follow instructions in the message in order to add the system monitor page to the *Trusted sites zone* before proceeding.

Working with System Monitor

Use the <, > and home icons to navigate the System Monitor.

From here you can view system information and create reports on:

- ***Management server:*** shows data on *your management server*
- ***Recording servers:*** shows data on *any number of recording servers* in your surveillance setup, which can be viewed per:
    - ***Disks***
    - ***Storage***
    - ***Network***
    - ***Cameras***
- ***Failover servers:*** shows data on *any number of failover servers* in your surveillance setup
- ***Additional servers:*** shows data on *log servers, etc*. in your surveillance setup
- ***Cameras:*** shows data *on any camera in any camera group* in your surveillance setup.

Each of these corresponds to a clickable, expandable area, most of which contains sub-areas. Each sub-area represents a server. When clicked, they provide relevant dynamic data on this server.

The *Cameras* bar however, contains a list of camera-groups to select from. Once a group is selected, you can select a specific camera and see dynamic data for it.

All servers display **CPU usage** and **available memory** information. Furthermore, recording servers also display **connection status** information.

Within each view, you can find a *History* link. Click it to view historic data and reports (to view reports on a camera, click the name of the camera). For each historic report, you can view data for the last 24 hours, 7 days or 30 days.

If you want to save and/or print reports, click the *Send to PDF* icon.

About Current Task

To get an overview of tasks under a selected recording server, their begin time, estimated end time and progress, do the following:

From the Site Navigation pane (see "Panes Overview" on page 36), expand *System Dashboard*, and click *Current Task*.

In general, all information showed in *Current Tasks* are snapshots and are refreshed by clicking on the refresh button in the lower right corner of the *Properties* pane.

About Configuration Report

When creating RC-E pdf configuration reports, you can include any possible elements of your RC-E system which you want to see in the report. Examples of what can be included ranges from licenses over device to alarm configuration, and much more.

Furthermore, you can customize your font and page setup and include a customized front page as listed:

Creating a Configuration Report

1. From the Site Navigation pane, expand *System Dashboard* and click *Configuration Reports*. This brings up the report configuration page.

2. Select the elements that you want to include in your report.

3. Optional: Click *Front Page...* to customize your front page. In the window that appears, fill in the needed info.

   Remember to select *Front page* as an element to include in you report, otherwise the front page you customize will not be included in your report.

4. Click *Formatting...* to customize your font, page size and margins. In the window that appears, select the wanted settings.

5. When you are ready to export, click *Export...* and select a name and save location for you report.

Tip: Remember, not all fonts support all special characters. If you have trouble viewing your special characters, try selecting a different font.

Configuration Report Details

The following buttons are available when setting up reports:

- ***Select All:*** Selects all elements in the list
- ***Clear All:*** Clears all elements in the list
- ***Front Page...:*** Opens a dialog allowing you to customize the front page

- **_Formatting..._:** Opens a dialog allowing you to format the report
- **_Export..._:** Opens a dialog allowing you to select the save location for the report and create the pdf.

Server Logs

Manage Logs

In the Management Client, you are able to view and copy contents from different logs related to the management server. The different logs have different purposes:

- Audit Log records user activity.
- Event Log records event-related information (see "Events Overview" on page 128).
- Rule Log records rules (see "Manage Rules" on page 133) in which the *Make new <log entry>*action (see "Actions and Stop Actions Overview" on page 110) has been specified.
- System Log records system-related information.

OnSSI RC-E has a number of default settings related to the different logs, see Handling Log Settings (on page 161). Furthermore, you are able to view logs in a number of different languages, export them, and save the exported logs as tab delimited text (.txt) files at a location of your choice; see Exporting Log (on page 160).

Viewing Log

To view a log, expand the *Management Server Logs* item in the Management Client's Site Navigation pane (see "Panes Overview" on page 36), then select the appropriate log.

Reading and Copying Log Content

Each row in a log represents a log entry. A log entry contains a number of information fields which are listed and briefly explained. Note, it is also possible to double-click any row and have all its details presented in a Log Details window. From the Log Details window, it is also possible to copy/paste any log contents:

- ***Level***
  - **All logs:** Display an icon indicating the level of the log entry.
- ***UTC Time***
  - **All logs*:*** Timestamp in coordinated universal time (UTC), an international high-precision time standard.
- ***Local Time***
  - **All logs:** Timestamp in the local time of the RC-E server.
- ***Description***
  - **All logs:** Description of the logged incident.
- ***Source Type***

  - **Rule Log only:** Type of equipment on which the logged incident occurred. Since log entries are administrator-defined and relate to incidents on the OnSSI RC-E system, source type will normally be *System*.
  - **Event and System Logs only:** Type of equipment on which the logged incident occurred, for example *Management Server* or *Device*.
  - **Audit Log only:** Type of equipment on which the logged incident occurred. Since remote user access is handled by the RC-E management server, source type will typically be *Server*.
- ***ID***
  - **All logs:** Identification number of the logged incident.
- ***Event Type***
  - **All logs, except Audit Log:** Type of event represented by the logged incident.

    Tip: For more information about event types, see also the events overview (on page 128).
- ***Source Name***
  - **All logs:** Name of the management server, device, etc. on which the logged incident occurred.
- ***Service Name***
  - **Event and Rule Logs only:** Name of service on which the logged incident occurred.
- ***Audit Type***
  - **Audit Log only:** Type of logged incident.
- ***Granted***
  - **Audit Log only:** Information about whether the remote user action was allowed (granted) or not.
- ***User***
  - **Audit Log only:** User name of the remote user causing the logged incident.
- ***Location***
  - **Audit Log only:** IP address or host name of the computer from which the remote user caused the logged incident.
- ***Rule Name***
  - **Rule Log only:** Name of the rule triggering the log entry.
- ***Generator Type***
  - **Rule Log only:** Type of equipment on which the logged incident was generated. Since the log entries are administrator-defined and relate to incidents on the RC-E system, generator type will normally be *System*.
- ***Generator Name***
  - **Rule Log only:** Name (if any) of the equipment on which the logged incident was generated.

Navigating Log

If a log contains more than one page of information, you are able to navigate between the log's pages by clicking the buttons in the bottom right corner of the log pane.

Furthermore, in the lower left corner lets you jump to a specific date and time in the log.

Searching Log

To search a log, use the *Search criteria* box in the top part of the log pane:

1. Specify your search criteria by selecting the required user name, location, etc. from the lists.

   Tip: You can combine selections, or make no selection in certain lists, as required. The more search criteria you combine, the less search results you will typically get.

2. Click *Refresh* to make the log page reflect your search criteria.

   Tip: To clear your search criteria, and return to viewing all of the log's content, click *Clear*.

Exporting Log

You are able to export logs, and save the exported logs as tab delimited text (.txt) files at a location of your choice.

You are able to target the exported log content by specifying which log, which log elements, and which time range to include in the export. For example, you are able to specify that only the System Log's error-related log messages from between January 2nd 2007 08:00:00 and January 4th 2007 07:59:59 should be included in your export.

To export a log, do the following:

1. Expand the *Management Server Logs* item in the Management Client's Site Navigation pane (see "Panes Overview" on page 36), and select the required log.

2. If you want to target the exported log's content, select the required criteria in the *Search criteria* section above the log. For example, you may select that your export should only contain log messages at a particular level, such as errors or warnings.

   Remember to click *Refresh* to make the log page reflect your selected criteria.

3. In the Management Client's menu bar, select *Action* > *Export Log...* This will open the *Export Log* window:

4. In the *Export Log* window's *Filename* field, specify a name for the exported log file.

   By default, exported log files will be saved in your *My Documents* folder. However, you are able to specify a different location by clicking the browse button next to the field.

5. Any criteria you have selected in order to target the content of the exported log will be listed in the *Filters* field. The field is non-editable; if you find that you need to change your criteria, close the window, and repeat steps 2-4.

6. Specify the time period you want the export to cover. You do this by specifying the required boundaries in the *Start date and time* and *End date and time* fields respectively. By clicking the arrow, you are able to select the required date from a calendar.

   To specify an exact time, overwrite the required time elements (hours:minutes:seconds) with the required values. In this example, the hours element is being overwritten.

   Tip: When you have selected time elements in order to overwrite them, you are also able to use your keyboard's UP ARROW and DOWN ARROW keys to increase/reduce the numbers in increments of one unit.

7. Click *Export* to export the required log content to the required location.

Handling Log Settings

OnSSI RC-E has a number of default settings related to its logs. To verify or change these settings, do the following:

1. Go to the Management Client's menu bar, and select *Tools > Options...*
2. In the *Options* window, select the *General* tab. One of the tab's settings applies for all types of logs:
   - ***Number of log rows to retrieve per page*:** Lets you specify the number of log rows you want to view on a single log page. If a log contains more than the specified number of rows, you will be able view the remaining rows on subsequent log pages.
3. Go to the *Options* window's *Management Server Logs* tab.

   In the tab's left box, select the required log. The selected log's settings are displayed in the tab's right box:
   - ***Log enabled:*** Lets you enable/disable the selected log. By default, all logs are enabled.

     The *System Log* and *Audit Log* cannot be disabled by clearing the box.
   - ***Days to keep log entries:*** Lets you specify how many days the log's information should be kept for. Default is 365 days.

     Excess log content will be deleted if the log reaches its maximum allowed size (see *Maximum number of entries*) before the specified number of days is reached.
   - ***Maximum number of entries*:** Lets you specify the maximum size of the log. Default is one million entries.

     Excess log content will be deleted if it reaches its maximum allowed age (see *Days to keep log entries*) before the specified number of entries is reached.

   For the *Audit Log*, you will furthermore see:
   - ***Enable user access logging*:** Lets you include detailed information about specific user actions in the audit log, e.g. about users' viewing of live video (and associated audio), PTZ actions, activation of output and events, export, playback of video and audio, use of playback features, any denied access to features, etc.
   - ***Playback sequence logging length:*** Lets you specify the number of seconds to pass for viewed images to be considered to be within the same sequence. Specifying a high number of seconds may help limit the number of viewed sequences logged, and thus reduce the size of the audit log.
   - ***Records seen before logging:*** Lets you specify the number of records to be viewed before logging the sequence.
4. Click *OK*.

RC-C

Manage RC-C Servers

The below information is for legacy reference only. Users of Ocularis need not utilize master/slave relationships as recorders are defined in the Ocularis Base.

If your organization has RC-C or NetDVMS installations, you can integrate these servers into your RC-E solution. You do this by adding the RC-C or NetDVMS servers through the RC-E Management Client.

Integration only works with RC-C servers running NetDVMS version 6.0 or later or RC-C 7.0 or later. Integration is not possible if your RC-E system uses IPv6. For the remainder of this section, the term RC-C will encompass supported versions of NetDVMS.

When added, RC-C servers can send data and video to the RC-E surveillance system. You can compare added RC-C servers with recording servers and these will likewise be available for viewing in clients.

Note that roles defined in RC-E's Management Client can be given access to data from RC-C servers. This is done by coupling RC-E roles with OnSSI RC-C user rights.

Furthermore, RC-C servers added in the RC-E Management Client will be listed in the *Add/Remove RC-C Servers* dialog which you can open by selecting *RC-C Servers...* from the *Tools* menu.

OnSSI RC-C's Recording Server service must be running for RC-E to receive data from the RC-C installation. See the RC-C documentation for more information.

Limitations when Adding RC-C Servers

There are a few limitations to how RC-C servers will work when added as slaves to the RC-E surveillance system. They will provide operational status and status details on cameras and RC-C servers but not on any other device types.

Also, you cannot define cameras, user rights, scheduling, or other settings for the RC-C installation, or see previews of the cameras in RC-E. All necessary RC-C settings must be made in RC-C's *Administrator* application or other relevant RC-C applications. See the RC-C documentation for more information.

The above is for legacy reference only. Users of Ocularis need not utilize master/slave relationships as recorders are defined in the Ocularis Base.

Prerequisites for Access Roles for RC-C Servers

On the RC-C server, check to see if one of the RC-C users has user rights that can be used in connection with an RC-E role.

Write the RC-C user's user name and password or Windows account down. You will need this information when you use RC-E's Management Client to define roles with access to RC-C servers. Note that user names and passwords are case sensitive.

You can also create a new user in RC-C, and assign the required user rights in RC-C, so they match the RC-E role. See the RC-C documentation for more information about creating new users in RC-C.

The above is for legacy reference only. Users of Ocularis need not utilize master/slave relationships as recorders are defined in the Ocularis Base.

Defining Access Roles for RC-C Servers

The below information is for legacy reference only. Users of Ocularis need not utilize master/slave relationships as recorders are defined in the Ocularis Base.

To give access to data from RC-C servers, do the following in the RC-E Management Client:

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Security,* and select *Roles*.
2. Select the required role from the list. If you want to define a new role, see About Roles (on page 145) for more information.
3. At the bottom of the *Role Settings* pane select the *RC-C Servers* tab.
4. Select the RC-C server to which you want to assign the role.
5. Select a user with the RC-C user rights that represent the correct user rights for the RC-E role you are assigning it to. You can do this in two ways:
   - In the *Basic Authentication* section, enter the user name and password for a user which is defined as basic authenticated user in RC-C.

     or -
   - In the *Windows Authentication* section, enter the Windows account name for a user which is defined as a Windows authenticated user in RC-C.

   Tip: If in doubt whether a user is defined as a Basic or Windows authenticated user in RC-C, open the *Image Server Administrator* window on the OnSSI RC-C server, and click *User Setup....* See the RC-C documentation for more information

   The selected RC-C user has not automatically been assigned to the role in question through RC-E's Management Client. The user's RC-C user rights have just been borrowed by the role, but the actual user has not been assigned to the role.

   OnSSI RC-E does not verify that the specified user name or password is correct or that the specified user name, password or Windows account name correspond to a defined user in RC-C. Therefore, make sure that you enter the information correctly. Note also that user names and passwords are case sensitive.
6. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

Adding RC-C Servers

The below information is for legacy reference only. Users of Ocularis need not utilize master/slave relationships as recorders are defined in the Ocularis Base.

To add an existing RC-C installation to your RC-E system, do the following:

1. From the RC-E Management Client's *Tools* menu select RC-C *Servers...*
2. In the *Add/Remove RC-C Servers* dialog click *Add...*.
3. Enter the IP address or the host name of the required RC-C server in the *RC-C server IP / Host name* field.
4. Enter the port number used by the RC-C server's Image Server in the *Port number* field.

Tip: The default port number is 80; if in doubt, you can find the port number in the *Image Server Administrator* window on the RC-C server.

5. Now enter information about the administrator of the RC-C server. You can do this in two ways:

   - Select *Windows* and click the browse button to the right of the *User name* field to use the Windows authentication method which authenticates the administrator through the administrator's Windows login.

   - or -

   - Select *Basic* and enter the RC-C administrator's user name and password in the *User name* and *Password* fields.

The reason why it is important that you enter the RC-C administrator information, is that you as administrator then will have unlimited rights to data from both RC-E and the RC-C installation.

The connection to the RC-C server is now established, but no roles in the RC-E Management Client—except the Administrator role—have been given access to data from the RC-C server. See Defining Roles with Access to RC-C Servers (see "Defining Access Roles for RC-C Servers" on page 163) for more information about giving users access to data from added RC-C servers.

Remember to define the network configuration settings, so the RC-E management server will be able to handle the token authentication of clients for added RC-C servers.

In the RC-E Management Client, you must add all RC-C servers you would like to receive data from. The RC-C system's internal master/slave setup cannot be reused by RC-E.

OnSSI RC-C Server Network Configuration

With the network configuration settings you specify the RC-E management server's server address so that the RC-E management server can handle the token authentication of clients for added RC-C servers.

From the RC-E Management Client's *Tools* menu select RC-C *Servers...*

1. In the *Add/Remove Registered Services* window, click *Network*...
2. Specify the LAN and/or WAN IP address of the OnSSI RC-E management server.

   If all involved servers (both the OnSSI RC-E management server and the trusted servers or the required OnSSI RC-C) are on your local network, you can simply specify the LAN address. If one or more involved servers access the system through an internet connection, you must also specify the WAN address.
3. Click *OK*.

Editing RC-C Servers

1. From the RC-E Management Client's *Tools* menu select RC-C *Servers...*
2. Select an RC-C server from the list, and click *Edit...* in the *Add/Remove RC-C Servers* dialog.
3. Edit the relevant settings and click *OK.*

Registered Services

Manage Network Configuration

1. In the *Add/Remove Registered Services* window, click *Network*...
2. Specify the LAN and/or WAN IP address of the OnSSI RC-E management server.

   If all involved servers (both the OnSSI RC-E management server and the trusted servers or the required OnSSI RC-C) are on your local network, you can simply specify the LAN address. If one or more involved servers access the system through an internet connection, you must also specify the WAN address.
3. Click *OK*.

For more details, see Manage Registered Services (on page 165) and Manage RC-C Servers (on page 162).

Manage Registered Services

Occasionally, you have servers and/or services which should be able to communicate with RC-E even though they are not directly part of the RC-E surveillance system.

You can manually specify servers/services as registered services in the Management Client:

Accessing Registered Services Configuration

1. In the Management Client's menu bar, select *Tools* > *Registered Services...*
2. The *Add/Remove Registered Services* window opens. From this window you can manage registered services.

Adding and Editing Registered Services

1. In the *Add/Remove Registered Services* window, click *Add...* or *Edit...*, depending on your needs.
2. In the *Add Registered Service* or *Edit Registered Service* window (depending on your earlier selection), specify or edit the following:
   - ***Service type*:**Pre-filled field.
   - ***Name*:** Name of the registered service; the name is only used for display purposes in the Management Client.
   - ***Description*:** Description of the registered service; the description is only used for display purposes in the Management Client.
   - ***URLs*:** Click *Add* to add the IP address or hostname of the registered service in question. If specifying a hostname as part of a URL, the host in question must exist and be available on the network. URLs must begin with *http://* or *https://* and must not contain any of the following characters: < > & ' " * ? | [ ] ".

     Example of a typical URL format: http://ipaddress:port/directory (where port and directory are optional).

     Note that you can add more than one URL if required.

- ***External*:** Select if the registered service connects to the management server with a public IP address.
- ***Trusted*:** Select if the registered service should be trusted immediately (this is often the case, but the option gives you the flexibility to add the registered service and then mark it as trusted by editing the registered service later).

  Note that changing the trusted state will also change the state of other registered services sharing one or more of the URLs defined for the registered service in question.

3. Click *OK*.

Network Configuration

With the network configuration settings you specify the RC-E management server's server LAN and WAN addresses in order for the RC-E management server and the trusted servers to be able to communicate.

1. In the *Add/Remove Registered Services* window, click *Network*...
2. Specify the LAN and/or WAN IP address of the OnSSI RC-E management server.

   If all involved servers (both the OnSSI RC-E management server and the trusted servers or the required OnSSI RC-C) are on your local network, you can simply specify the LAN address. If one or more involved servers access the system through an internet connection, you must also specify the WAN address.
3. Click *OK*.

Important Prerequisites When Running Federated Sites

The easiest way to make federated architecture work correctly is to prepare your RC-E system for this feature during installation. There are certain important prerequisites that you must ensure already at the time of installing your management server. This can be done in different ways - choose between the procedures in alternative 1-3:

Alternative 1: Connect Sites from the Same Domain (with Common Domain User) and Customize the Installation of the Management Server to the Federated Architecture

Before installation of the management server, a common domain user should be created and used as the administrator on all computers involved in the federated architecture. Depending on whether you select *Custom* or *Typical* during installation of the management server, make sure to select the appropriate procedure. Note that a typical installation requires more configuration on all sites before federated will work properly.

Custom installation:

1. Start the management server installation (see "Install Management Server" on page 13) and select *Custom*.
2. Select to install the Management Server service using a user account.

   The selected user account must be the administrator on all management servers and must also be used when installing the other management servers in the federated setup.
3. Finish the installation.
4. Repeat steps 1-3 to install any other RC-E systems you want to connect in the federated architecture.
5. See Adding a Site to the Hierarchy (see "Manage OnSSI Federated Architecture" on page 177) for details on how to proceed.

Typical Installation - set up *Network Service* on all servers:

1. Start the management server installation (see "Install Management Server" on page 13) and select *Typical*, let it run till it finishes.

This will install the management server as a *Network Service*.

2. Repeat step 1 to install any other RC-E systems you want to connect with the federated architecture.
3. Using a Management Client, connect to the management server you want to have as your parent site.
4. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Security*, click *Roles,* and in the overview pane (see "Panes Overview" on page 36), click *Administrator*.
5. Add the child computer to this parent server's *Administrator* role. See Assign and Remove Users and Groups to/from Roles (on page 149) for details.
6. Log out of the parent management server and connect to the management server that you just added as a child.
7. Once again, in the overview pane (see "Panes Overview" on page 36), click *Administrator*.
8. Add the parent computer to this servers *Administrator* role. See Assign and Remove Users and Groups to/from Roles (on page 149) for details.
9. Log out of the management server, connect to the parent management server, and see Manage OnSSI Federated Architecture (on page 177) for details on how to proceed.

Alternative 2: Connect Sites From Different Domains

To make it possible to connect sites across domains, it is very important that these domains are trusted by each other. Setting up domains to trust each other has nothing to do with federated architecture but is entirely a matter of Microsoft Windows Domain configuration.

For further information on how to set up trusted domains, see Microsoft website: http://technet.microsoft.com/en-us/library/cc961481.aspx **(**http://technet.microsoft.com/en-us/library/cc961481.aspx**).**

1. When the domains, on which the sites you want to connect to each other in a federated architecture, are trusted correctly, follow the same instructions as if only one domain was present (see Alternative 1).

Alternative 3. Connect Sites in Workgroup(s)

When you connect sites inside workgroups, it is an important prerequisite for federated architecture to work correctly that the same administrator account is present on all computers you want connected in the federated architecture. This must be in place before installing RC-E.

1. Log in to *Windows* using a common administrator account.
2. Start the management server installation (see "Install Management Server" on page 13) and click *Custom*.
3. Select to install the Management Server service using a common administrator account.
4. Finish the installation.
5. Repeat steps 1-4 to install any other RC-E systems you want to connect. They must all be installed using a common administrator account.
6. See Adding a Site to the Hierarchy (see "Manage OnSSI Federated Architecture" on page 177) for details on how to proceed.

It is **not** possible to mix domain(s) and workgroup(s), i.e. connect sites from a domain to sites from a workgroup and vice versa.

Options

Options

The Management Client's *Options* dialog lets you specify a number of settings related to the appearance of the application, to logging, to mail server configuration, etc.

You access the *Options* dialog from the Management Client's menu bar (see "Management Client Overview" on page 34), by selecting *Tools* > *Options*.

The *Options* dialog features the following tabs:

General

The *General* tab lets you specify the following:

- ***Number of log rows to retrieve per page:*** Lets you select the number of log rows you want to view on a single log page. Default is 50 rows. If a log contains more than the specified number of rows, you will be able view the remaining rows on subsequent log pages.
- ***Default preview frame rate*:** Lets you select which frame rate to use for the thumbnail camera images displayed in the preview pane (see "Panes Overview" on page 36). Default is 1 frame per second.

  Refreshing the Management Client' layout (by pressing F5 on your keyboard or selecting *Action* > *Refresh* from the menu bar) is required for a change to take effect.

  Note that a high frame rate (i.e. a high image quality) in combination with a large number of thumbnail images in the preview pane may slow the system down. You are able to limit the number of thumbnail images with the *Max. number of previews* setting.
- ***Max. number of previews*:** Lets you select the maximum number of thumbnail images displayed in the preview pane. Default is 64 thumbnail images.

  Refreshing the Management Client' layout (by pressing F5 on your keyboard or selecting *Action* > *Refresh* from the menu bar) is required for a change to take effect.

  Note that a large number of thumbnail images in combination with a high frame rate (i.e. a high image quality) may slow the system down. You are able to limit the frame rate used for the thumbnail images with the *Default preview frame rate* setting.
- ***Motion detection 'on' when adding camera devices*:** Lets you select whether motion detection should be enabled while cameras are being added to a recording server through the *Add Hardware* (see "*Add Hardware (Cameras, etc.)*" on page 49) wizard.

  Select check box to enable motion detection while using the wizard (default).

  Note that this setting only applies while*Add Hardware* is in use. When the wizard is not in use, motion detection will be active for all cameras for which it has been enabled, regardless of this setting.

  Why would I want to disable motion detection while using Add Hardware? Motion detection is a key element in the surveillance system, and is thus by default enabled for all cameras on the system. However, motion detection uses a relatively large amount of computing resources. If your system features a very large

number of cameras, and motion detection is enabled on all cameras, the system may thus be slowed down slightly, and adding of new cameras may take longer than usual. In order to be able to add new cameras as quickly as possible, you therefore have the option or disabling motion detection while the wizard *Add Hardware* is used.

- ***Enable multicast live when adding camera devices*:** Lets you select whether multicast (see "Manage Multicasting" on page 70) should be enabled while cameras are being added to a recording server through the wizard Add Hardware.

  Select check box to enable multicast while using the wizard (default).

  Note that this setting only applies while*Add Hardware* is in use. When the wizard is not in use, multicast will be active for all cameras for which it has been enabled, regardless of this setting.

- ***Language**:* Lets you select which language your Management Client system should run.

- ***Timeout for PTZ sessions:*** Handling of PTZ cameras may be interrupted manually by Ocularis Client users with the necessary user rights. This setting lets you select how much time should pass before regular patrolling is resumed after a manual interruption. The setting will apply for all PTZ cameras on your OnSSI RC-E system.

- ***Ignore device communication errors if communication reestablished before:*** Lets you select how long a communication error may last without being logged by the system log—or in other words, when it is brief enough to be ignored.

Server Logs

The *Server Log* tab lets you specify settings for RC-E's five different management server logs.

See Manage Logs (on page 158) for more information.

Mail Server

The *Mail Server* tab lets you specify settings for the outgoing SMTP mail server you are going to use with your RC-E system.

See Outgoing SMTP Mail Server Settings (on page 171) for more information.

AVI Generation

The *AVI Generation* tab lets you specify compression settings for the generation of AVI video clip files. Specifying these settings is a prerequisite if you want to include AVI files in e-mail notifications sent out by rule-triggered notification profiles (see "Manage Notification Profiles" on page 141). See AVI Compression Settings (on page 170) for more information.

Network

The *Network* tab lets you specify local IP address ranges. See Manage Local IP Address Ranges (on page 171) for more information.

Bookmarks

The *Bookmarks* tab is not used in this version of RC-E.

User Settings

The *User Settings* tab lets you specify settings for user preference, such as whether a message should be shown when edge recording is enabled.

See *Record* tab Overview (on page 103) for more information.

AVI Compression Settings

You are able to specify compression settings for the generation of AVI video clip files. Specifying these settings is a prerequisite if you want to include AVI files in e-mail notifications sent out by rule-triggered notification profiles (see "Manage Notification Profiles" on page 141).

To specify compression settings for AVI file generation, do the following:

1. Go to Management Client's menu bar, and select *Tools* > *Options...*
2. In the *Options* window, select the *AVI Generation* tab.
3. Specify the following:
   - ***Compressor***: Select the required codec (compression/decompression technology).

     Tip: If in doubt about which codec to select, try using Indeo® 5.10 (if available). This codec generally provides a good compromise between quality and file size.

     Tip: For some but not all codecs you are able to configure them by clicking *Configure...*. Configuration options are entirely codec-specific. And also view detailed information about version number etc. by clicking *About...*.
   - ***Compression quality***: (Not available for all codecs). Use the slider to select the required degree of compression (*0-100*) to be performed by the codec.

     0 means no compression, generally resulting in high image quality and large file size. *100* means maximum compression, generally resulting in low image quality and small file size.

     If the slider is not available, compression quality will be determined entirely by the selected codec.
   - ***Key frame every***: (Not available for all codecs). If you want to use key frames, select the check box and specify the required number of seconds between keyframes in the neighboring field.

     A keyframe is a single frame stored at specified intervals. The keyframe contains the entire view of the camera, whereas the following frames contain only the pixels that change. This helps greatly reduce the size of files.

     If the check box is not available, or not selected, every frame will contain the entire view of the camera.
   - ***Data rate***: (Not available for all codecs). If you want to use a particular data rate, select the check box and specify the required number of kilobytes per second in the neighboring field.

     If the check box is not available, or not selected, date rate will be determined entirely by the selected codec.
4. Click *OK*.

Outgoing SMTP Mail Server Settings

You are able to specify settings for the outgoing SMTP mail server you are going to use with your RC-E system. Specifying these settings is a prerequisite for using rule-triggered notification profiles (see "Manage Notification Profiles" on page 141) to send out e-mail notifications on events, etc.

Note that when using the SMTP Service with .NET 4.0, it is not possible to send attachments over 3 MB. However two hotfixes (must be run in the listed order) from Microsoft can be found at:

http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226 (see http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226 - http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=30226)

http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723 (see http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723 - http://connect.microsoft.com/VisualStudio/Downloads/DownloadDetails.aspx?DownloadID=31723)

1. Go to the Management Client's menu bar, and select *Tools* > *Options...*
2. In the *Options* window, select the *Mail Server* tab
3. Specify the following:
   - ***Sender e-mail address:*** Type the e-mail address you want to appear as the sender of e-mail notifications for all notification profiles. Example: sender@organization.org.
   - ***Outgoing mail (SMTP) server name***: Type the name of the SMTP mail server which will be used for sending e-mail notifications for all notification profiles. Example: mailserver.organization.org.

     Furthermore, if the SMTP mail server requires login, select *Server requires login*, and type the required user name and password.
4. Click *OK*.

TLS (Transport Layer Security) and its predecessor SSL (Secure Socket Layer) is not supported; if the sender belongs on a server that requires TLS or SSL, e-mail notifications will not work properly. Also, you may be required to disable any e-mail scanners that could prevent the application sending the e-mail notifications.

Tip: When you add new notification profiles, you will be able to send test e-mails and thus verify that your SMTP mail server settings are correct.

Manage Local IP Address Ranges

Client users may connect from the local network as well as from the internet, and in each case the surveillance system should be able to provide suitable addresses so the clients can get access to live and recorded video from the recording servers:

When clients connect locally, the surveillance system should reply with local addresses and port numbers.

- When clients connect from the internet, the surveillance system should reply with the recording servers' public addresses (see "Manage Public Addresses" on page 72), i.e. the address of the firewall or NAT (Network Address Translation) router, and often also a different port number (which is then forwarded to recording servers).

The surveillance system must therefore be able to determine whether a client belongs on a local IP range or on the internet. For this purpose, you are able to define a list of IP ranges which the surveillance system should recognize as coming from a local network.

Working with Local IP Address ranges...

1. In the Management Client's menu bar, select *Tools* > *Options*. This will open the Options dialog (see "Options" on page 168).

   Tip: You can also access the *Options* dialog from the *Network* tab; this can be handy if you are also configuring the public IP address of a recording server.

2. In the *Options* dialog, select the *Network* tab.

Defining Local IP Address Ranges

a On the *Network* tab, click *Add*.

b In the *Range Start* column, specify the first IP address in the required range. Then specify the last IP address in the range in the *Range End* column.

Tip: If required, a range may include only one IP address (example: 192.168.10.1-192.168.10.1).

c If more ranges are required, repeat steps a - b.

d Click *OK*.

Editing Local IP Address Ranges

a Overwrite the existing information in the *Range Start* and *Range End* columns as required.

b Click *OK*.

OnSSI Federated Architecture

OnSSI Federated Architecture Overview

OnSSI Federated Architecture allows multiple individual standard RC-E systems (also known as sites) to interconnect in a parent/child hierarchy of sites.

IMPORTANT: Federated hierarchy is only possible with RC-E 4.0 or newer. Before installing RC-E, see Important Prerequisites When Running Federated Sites (on page 166).

In this text, the term *parent* refers to a parent site and *child* to a child site.

Through federated architecture, client users—based on their user rights—have seamless access to video, audio and other resources across individual RC-E sites. In addition, through a single login, administrators can centrally manage all sites within the federated hierarchy—again based on administration rights for the individual sites.

As it provides unlimited scalability, flexibility and accessibility to video surveillance across multiple sites and has no limit to the number of sites you can add, federated architecture is well suited for large installations covering multiple buildings, campuses, or entire city areas.

Each site in a federated hierarchy is installed and configured as a normal stand-alone system with standard system components, settings, rules, schedules, administrators, users, and user rights. Once each site has been installed, these can be connected by requesting a federated architecture link from one site (the parent) to another (the child). When the link is established, the two sites automatically create a federated architecture hierarchy to which more sites can be added to grow the federated hierarchy.

Illustration of OnSSI Federated Architecture (on page 177)

In this example, the federated architecture hierarchy consists of six sites. As illustrated, each site can be both a parent and a child at the same time thus making it possible to create a hierarchy with as many levels as needed. It is also evident that a site can link to several child sites on the same level in a hierarchy.

Once a federated hierarchy is created, it allows users and administrators logged in to a site, to access that site and any child or sub-child sites it may have. Access to child and sub-child sites in the hierarchy is not gained automatically, but dependent on appropriate user and administrator rights.

It is only relevant to speak of a parent/child setup for management servers—not for recording servers (see "The RC-E Server (Management Server)" on page 7). However, due to their relations to management servers, recording servers will automatically become part of the parent/child setup.

See Manage OnSSI Federated Architecture (on page 177) for details on how to work with federated architecture.

Licensing of OnSSI Federated Architecture

To learn about licensing in general, see Manage Licenses (on page 45).

Federated Architecture can be used - freely - within the **same legal entity** as many times as needed. In a federated architecture, all sites share the same Software License Code (SLC) and device licenses are shared between all sites.

In the case of **different legal entities** running a federated architecture, each system requires a valid set of base and device licenses. Furthermore, in order for a device to be accessible across a federated setup, one *OnSSI Federated Architecture Device License* is required per device accessed in the federated site.

To get additional licenses for your RC-E system, contact your OnSSI vendor..

Basic Rules of Federated Sites

One Parent-Many Children

A child can only have one parent, but a parent can have an unlimited number of children.

Parent Requests Child, Not the Other Way Around

A new parent/child link is always requested by the parent, and if necessary, authorized by the child. See Accepting Inclusion in the Hierarchy (see "Manage OnSSI Federated Architecture" on page 177).

One Level at the Time

A parent knows about all its children, children's children, etc., but only controls them one level down. Furthermore a child only knows about and answers to its parent one level up.

Synchronization of Hierarchy

A parent always contains an updated list of all its currently attached children, children's children, etc. But when distant communication is needed, it takes place level by level, each level forwarding and returning communication, until it reaches the server requesting the information. Depending on the number of levels that must be updated, changes to a hierarchy might take a little time to become visible in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36), see Refreshing the Site Hierarchy (see "Manage OnSSI Federated Architecture" on page 177). The federated hierarchy has a regularly scheduled synchronization between sites, as well as management-triggered synchronization every time a site is added or removed. This synchronization only contains site configuration data and each time will send less than 1MB. In addition to the data sent during synchronization, video or configuration data will be sent when a user or administrator views live or recorded video or configures the system. The amount of data in this case depends on what and how much is being viewed. It is not possible to schedule your own synchronizations.

Principles for Setting Up Federated Sites

When working with federated architecture, the link between management servers is established from the management server wanting to become parent to another management server. Theoretically, establishment of a parent/child relationship happens as follows:

1. The parent sends a link request to the potential child.
2. Depending on administrator settings, the child might have to authorize the link request.
3. If necessary, the child authorizes the link request.
4. Relevant info is exchanged.
5. The new parent/child link is established.

The Administrator Role and Federated Sites

- **Administrator vs. Non-administrator**

  In general, you must be an administrator to work with federated architecture. However, by requesting the adding of children to a top-site (to which you have administrator rights), you can (without administrator rights to the other sites) create the overall initial infrastructure of a federation. But, as described in Manage OnSSI

Federated Architecture (on page 177), the administrator of each individual child must later authorize the connection before it can take effect.

- **Becoming an Administrator Using Active Directory-Two Possible Scenarios**

  How to become administrator of an OnSSI Federated Architecture setup using Active Directory depends on how the management server is installed. If it is installed as described in either of the following two scenarios, you gain administrator rights of the entire setup. Otherwise not.

  - If the management server is installed as a **Network Service:** Both/All computers involved must be added as users to each other's RC-E administrator role before a parent/child link can be established without acceptance from the administrator of the child. See Assign and Remove Users and Groups to/from Roles (on page 149) for details. This type of setup is primarily recommended if all sites in the hierarchy are not a member of the same Domain. See also Important Prerequisites When Running Federated Sites (on page 166).
  - If the management server is installed as a **user account:** This user account must be a member of the administrator group of the server being linked to before one or more parent/child link(s) can be established without acceptance from the administrator of the child. This type of user right setup is primarily recommended if the number of sites in a hierarchy is large. See also Important Prerequisites When Running Federated Sites (on page 166).

- **Becoming an Administrator Using Work Groups**

  How to become administrator of a federated architecture setup using work groups depends on how accounts are created. If they are set up correctly, you gain administrator rights of the entire setup. Otherwise not. See Important Prerequisites When Running Federated Sites (on page 166) for details on how to do this.

If the previous criteria are not met, the administrator of a child must accept requests for inclusion in the hierarchy (see "Manage OnSSI Federated Architecture" on page 177) manually before links can be established.

One or More Administrators?

An OnSSI Federated Architecture setup can have many administrators working on it at the same time. Furthermore, the *Site Navigation* pane is dynamic and reflects changes to the federated site made both by you and possibly other administrators. This means that you might see changes here caused by other users. You might also experience that a site you are connected to is removed from the federated site by another user. In this case, your site will be removed from the *Federated Site Hierarchy* pane, but nothing will change in the *Site Navigation* pane or elsewhere, allowing you to continue working.

Possibilities and Constrains of Federated Sites

In principle, there is no limit to the number of sites you can add to a federated architecture and how these can be linked, offering you unlimited scaling, flexibility and accessibility.

Frequently Asked Questions to Federated Sites

What is a federated site? A federated site is basically just an individual RC-E system, complete with management server, SQL server, one or more recording server(s), failover server(s) and cameras. To make use of OnSSI Federated Architecture, you must connect at least two individual RC-E systems. The Management Client (on page 34) is used to configure federated hierarchies. In principle, it lets you connect to any site in the federated hierarchy at any given time (if user rights permit) using the log in credentials for your home-site. This offers you a central overview, and, at the same time, lets you zoom in on selected sites by connecting to a specific site to have a closer look, make configurations, or carry out maintenance. Note however, that the Management Client is only able to see other sites from the level of the site you are logged into and downwards in the hierarchy.

What is a top-site? Your top-site is the top level management server of your entire OnSSI Federated Architecture setup.
An example an organization could have a top-level server called *MyCorp*. Second level servers called *MyCorp/RegionalServers*. Third level servers called *MyCorp/ReginalServers/CityNames*. And so on. In this case, *MyCorp* is your top-level server. There can only be one top-level server.

Tip: In a federated hierarchy, it is always a good idea to name your servers in a recognizable way, for example, using regional names or names implying where/in what context the server is located. Using, for example, consecutive numbers only, might be confusing if you have many servers.

What is a home-site? Your home-site is the site to which you are logged in. Since you may be logged in far down in the hierarchy, this is not necessarily the same as your top-site—but it **may** be. You are only able to see children from the point at which you are logged in and downwards.

Can a site be both a parent and a child at the same time? Yes, a parent with children attached, can easily be child to another site, and vice versa. This is because the parent/child concept is relative and used only in respect to other specified servers. So when looking at the OnSSI Federated Architecture illustration (see "Illustration of OnSSI Federated Architecture" on page 177), site 7 is the parent of site 8, but the child of site 6.

What is the difference between logging into and connecting to a site? To work with OnSSI Federated Architecture you must always be logged in to a site via the Management Client. You can log in to any site if you have administrator rights to that particular site. This is called your home-site. When logged in to your home-site, you can see all its children (if user rights permit). From your home-site you can also connect to its children (if user rights permit). Embedded in the connection process is an automated and seamless log-in, using the same credentials as your home-site log in. Connecting to a child allows you to see and work with that site (if user rights permit). However, even though technically you log out of your home-site when connecting to another site, you will still see the site structure as your (former) home-site sees it. This means, that any changes you make to a child might not be visible until such changes reaches your home-site via scheduled synchronization. So changes you make in your hierarchy might not be reflected in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36) until later. For more details, see Basic Rules of Federated Sites (on page 174).

You cannot refresh via a connection to a child, this but must take place directly from the home-site.

When do I need to accept link requests? Whether as the administrator of a child you must accept a link request or not (or the link request is accepted automatically) depends on your administrator settings. See Administrator Role and Federated Sites (see "The Administrator Role and Federated Sites" on page 174).

Where is OnSSI Federated Architecture configured and managed? Setting up and configuring OnSSI Federated Architecture takes place in the Management Client.

Do I need more than one Ocularis Client to work with OnSSI Federated Architecture? When working with OnSSI Federated Architecture, all work in the Ocularis Client can be handled from one Ocularis Client installation, i.e. there is no need for a one-to-one relationship between sites and Ocularis Clients.

How do I view video from federated sites? You can view video from federated sites in any Ocularis Client, i.e. there is no need for a one-to-one relationship between sites and Ocularis Clients. You will always get the view, i.e. see the site structure as the parent you are currently logged in to.

Can I include RC-C slave(s) in my federated hierarchy? Yes, that is possible, but only as slave(s) to an RC-E management server. In this case, the relationship with the RC-C server will work as described in Manage RC-C Servers. See also Defining Alarms for information on working with alarms in a federated setup.

Is OnSSI Federated Architecture the same as multiple management servers, a.k.a. clustering? No, OnSSI Federated Architecture is not the same as clustering. Clustering is a method of obtaining failover support for a management server on a site. With clustering, it is only possible to have one active management server per surveillance setup, but other management servers may be set up to take over in case of failure. On the other hand, OnSSI Federated Architecture is a method of combining multiple independent corporate sites into one large setup, offering flexibility and unlimited possibilities.

Federated Sites Example Scenario—Limestone City

The following is an example of how several RC-E systems can be integrated into a federated architecture-in this case in a **City Surveillance** scenario.

Many surveillance integrators want to integrate several independent surveillance entities into a large scale system, where each site can still be used and managed locally and users and administrators can be given access to the entire large scale installation.

In this example, several governmental and business installations must be tied together in a large scale system offering the different entities local access and management of the system, as well as governmental (police etc.) access in case of crimes and emergencies.

All entities must be connected to the city's video surveillance so that City Hall officials and police officers can access video from their business or residential area to monitor live video or investigate recorded video in case of break-ins, thefts, vandalism, emergencies, terror etc.

In addition to being connected to the city's video surveillance, A.C.M.E Industries Inc, Downtown Residential and Limestone Center Shopping Mall also want to segment their installation in several sites as they have several physical locations that they want to monitor. The segmented architecture offers them greater flexibility during installation and daily usage.

The city uses federated architecture, allowing the entities independent video surveillance while being tied into the city wide surveillance system at the same time.

Because the police have installations that City Hall should not have access to, the Police Headquarters is selected as the top-site in the city's federated surveillance hierarchy.

Each site is then tied into Limestone city's federated hierarchy as follows:

- **Level 1:** Police Headquarters.
    - **Level 2:** Limestone City.
        - **Level 3:** City Hall and **MB Industries as one group.**
            - **Level 4:C**entral Station, Streets & Intersections and Parks as one group under City Hall.
        - **Level 3:** Limestone Center Shopping, Downtown Residential, Limestone Transportation Ltd and A.C.M.E Industries Inc. as one group.
            - **Level 4:** Shops, Branch Malls and Residential area shops as one group under Limestone Center Shopping.
            - **Level 4:** Branch Office 1 and Branch Office 2 as one group under A.C.M.E Industries Inc.

Manage OnSSI Federated Architecture

For conceptual details on OnSSI Federated Architecture, see OnSSI Federated Architecture Overview (on page 173).

The RC-E Management Client has a Federated Sites Hierarchy pane (see "Panes Overview" on page 36) dedicated to displaying federated sites and their parent/child links. From the *View* Menu (see "Management Client Menu Overview" on page 40), you can show or hide the *Federated Sites Hierarchy* pane. The pane is located on the left side of the Management Client window, under the *Site Navigation* pane.

The parent server you are logged in to (your home-site), is always at the top of the site hierarchy. You can view all its linked children and downwards through the parent/child hierarchy. Settings and configurations of your home-site is always reflected in the *Overview* and *Properties* panes and its site-name visible at the top of the *Site Navigation* pane.

To connect to another site in the hierarchy (see "Connecting to Another Site in the Hierarchy" on page 180), click the wanted site in the *Federated Sites Hierarchy* pane.

What if I only have one server and don't run federated architecture? Your user interface looks the same, but when you view the *Federated Sites Hierarchy* pane you will only see the one server in your setup.

Expand/Collapse

You can expand and collapse a site in the *Site Navigation* pane, to see its children, if any.

Site Navigation Pane

The name, settings and configurations of the highlighted site (red arrow) are reflected in the *Site Navigation* pane.

Right-clicking is not Selecting!

Because you must be able to delete a site without being connected to it, **right-clicking a site does not select it,** but offers a context menu, which differs depending on where in the hierarchy you are. See Action Menu (see "Management Client Menu Overview" on page 40).

Context Menu

From the *Federated Site Hierarchy* pane, a context menu lets you add sites to a hierarchy, accept inclusion in a hierarchy, rename sites in a hierarchy, detach sites from hierarchy, work with site properties and refresh site hierarchy.

Due to the nature of federated sites, when the context menu is activated from a parent, you cannot accept inclusion in the hierarchy. And when it is activated from a child, it is not possible to refresh the site hierarchy.

Adding a Site to the Hierarchy

You can add children to both your home-site and to its children (when connected to them).

Prerequisites

To add a child to a parent in your hierarchy, one of the following two scenarios must be true:

- The management server is installed as a **Network Service:** Before a parent/child link can be established without the acceptance from the administrator of the child, both computers involved (parent and child) must be added as a user to the other's RC-E administrator role. See Assign and Remove Users and Groups to/from Roles (on page 149).
- The management server is installed as a **user account:** This user account must be a member of the administrator group of the server being linked to before a parent/child link can be established without the acceptance from the administrator of the child.

If neither of these criteria are met, the administrator of the child needs to accept the request for inclusion in the hierarchy (see "Accepting Inclusion in the Hierarchy" on page 179) before the link can be established. See OnSSI Federated Architecture Overview (on page 173) for more details**.**

To Add a Site to Hierarchy

1. In the *Management Client* window, in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36), select the relevant site, right-click, and click *Add Site to Hierarchy*.

Tip: As an alternative to using the menu, press the CTRL+N keys on your keyboard.

2. Insert the URL of the requested child in the *Add Site to Hierarchy* window.
3. Click *OK*.
4. A link to the new child site is added to the *Federated Sites Hierarchy* pane.
5. If you can establish the new child link without requesting acceptance from the administrator (see *Prerequisites* described earlier), skip to step 7.

   If **not**, the new child has the awaiting acceptance icon, see "Accepting Inclusion in the Hierarchy" on page 179 and its administrator must authorize the request.
6. Make sure the child's administrator authorizes the link request (this is done from the child site).
7. The new parent/child link is established and the *Federated Sites Hierarchy* pane is updated with the icon for the new child.

   Due to synchronization issues, any changes made to children located far from your home-site might take some time to be reflected in the *Federated Sites Hierarchy* pane. See Basic Rules of Federated Sites (on page 174).

Accepting Inclusion in the Hierarchy

You must accept a child link request manually if your administrator settings require this.

- If the management server is installed as a **Network Service:** Computers involved must **not** be added as users to each other's RC-E administrator role, but should be added as another RC-E **non**-administrator role. See Assign and Remove Users and Groups to/from Roles (on page 149).
- If the management server is installed as a **user account:** This user account must **not** be a member of the administrator role of the server being linked to.

Otherwise inclusion will take place automatically.

See also Administrator Role and Federated Sites (see "The Administrator Role and Federated Sites" on page 174).

Prerequisites

The potential child must have received a link request from the potential parent. As a result, the child has the awaiting acceptance icon.

To Accept Inclusion in a Hierarchy

1. In the Management Client window (of the potential child), in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36), select the relevant site, right-click, and click Accept Inclusion in Hierarchy.
2. Click *Yes*.
3. The new parent/child link is established and the *Federated Sites Hierarchy* pane is updated with the normal site icon for the selected site.

   Due to synchronization issues, any changes made to children located far from your home-site might take some time to be reflected in the *Federated Sites Hierarchy* pane. (see "OnSSI Federated Architecture Overview" on page 173), *Basic Rules of Federated Sites*, *Synchronization of Hierarchy.*

Connecting to Another Site in the Hierarchy

You can connect to all sites in your federated architecture if your administrator settings are correct.

Prerequisites

To connect from one site in your hierarchy to another, one of the following two scenarios must be true:

- The management server is installed as a **Network Service:** Both computers involved must be added as users to each other's RC-E administrator role. See Assign and Remove Users and Groups to/from Roles (on page 149).
- The management server is installed as a **user account:** This user account must be a member of the administrator group of the server being linked to.

See Administrator Role and Federated Sites section (see "The Administrator Role and Federated Sites" on page 174).

To Connect to Another Site in Hierarchy

Simply click the wanted site in the Federated Site Hierarchy pane (see "Panes Overview" on page 36). A brief dialog informs you that you are being connected to the new site. When connection is complete, your view in the *Federated Sites Hierarchy* pane will change to reflect that you are connected to a different site.

Do I log out of my home-site when I connect to another site in the hierarchy? Both yes and no. Embedded in your home-site log-in is an automated and seamless log-in to its children as well, using the same credentials as your home-site log-in. However, even though you technically log out of your home-site when connecting to one of its children, you still see the world as your (former) home-site sees it.

Detaching a Site from the Hierarchy

Detaching/Removing a site from its hierarchy involves two different results **depending on where in the federated architecture you are located**.

If you are within your hierarchy-except your home-site-this will detach the selected site from the rest of the hierarchy. You will no longer be able to see the detached site.

If, on the other hand, you are located at your home-site, your home site will be detached from the rest of the hierarchy including any sites located under your home-site. Your home-site becomes the new top-site.

Detach Child from Hierarchy(Location: Any site)

Prerequisites

The site you are detaching is any site, **except** your home-site.

To Detach Child from a Hierarchy

1. In the Management Client window, in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36), right-click the site you want to detach-**except** the home-site-select *Detach Site from Hierarchy*.
2. Click *Yes*.
3. The detached site is removed and the *Federated Sites Hierarchy* pane is updated.

Tip: You do not have to connect to a site to detach it. Just point your mouse to the relevant site and right click, select *Detach Site from Hierarchy*.

Detach Home-site from Parent Hierarchy(Location: Home-site, which has a parent)

Prerequisites

Your home-site must be the child of another site, i.e. have a parent.

To Detach Home-site from a Parent Hierarchy

1. In the *Management Client* window, in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36), right-click the **home-site**, and click *Detach Site from Hierarchy*.
2. Click *Yes*.
3. The *Federated Sites Hierarchy* pane is updated, your home-site becomes the new top-site, and the normal site icon changes to a top-site icon.
4. Click *OK*.

Due to synchronization issues, changes might take a little time to be reflected in the *Federated Sites Hierarchy* pane. See Basic Rules of Federated Sites *(on page 174).*

Tip: As an alternative to using the menu to detach from hierarchy, press the DELETE key on your keyboard.

Refreshing the Site Hierarchy

Automatic synchronizations happen regularly through all steps of your parent/child setup. But if you want a current overview of things, and do not want to wait for the next automatic synchronization, you can refresh.

When refreshing, the home-site will display a current overview of the state of things from the home-site's point-of-view.

Note that only changes saved by the home-site since the last synchronization will be reflected—changes further down in the hierarchy will not be reflected. For this, a full scheduled synchronization is needed.

1. In the *Management Client* window, in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36), right-click the home-site, and click select *Refresh Site Hierarchy*.
2. The *Federated Sites Hierarchy* pane is refreshed, reflecting any changes.

It is not possible to schedule your own synchronizations.

Renaming a Site

You can rename both your home-site and its children when connected to them.

1. In the Management Client, in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36), select the relevant site, right-click, and click *Rename Site*.

   Tip: As an alternative to using the menu, press the F2 key on your keyboard.
2. You can now overwrite the name of the site.
3. The *Federated Sites Hierarchy* pane is updated, reflecting the name-change.

Due to synchronization issues, any changes to remote children might take some time to be reflected in the Federated Sites Hierarchy pane. See Basic Rules of Federated Sites (on page 174).

Setting the Site Properties

You can view and, possibly, edit properties on your home-site and its children.

1. In the Management Client, in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36), select the relevant site, right-click, and select *Properties.*

2. If needed, change the following:

General Tab

Information related to the site you are currently connected to:

- ***Name**:* Enter the name of the site displayed in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36) and the *Site Navigation* pane.
- ***Description**:* Enter a description of the site.
- ***URLs**:* Use the list to add and remove URL(s) for this site and indicate whether they are external or not.
- ***Version:*** Version number of the site/management server.
- ***Service account:*** The service account under which the management server is running.
- ***Time for last synchronization:*** Last synchronization date.
- ***Status for last synchronization:*** Status of last synchronization. It can be either *Successful* or *Failed*. If failed, further information is offered.

Click *OK* to save changes.

Parent Site Tab(available on child sites only—marked in red)

Non-editable information regarding the parent of the child you are currently connected to:

- ***Name**:* Shows the name of the parent to be displayed in the Federated Sites Hierarchy pane (see "Panes Overview" on page 36) and *Site Navigation* pane.
- ***Description**:* Shows a description of the parent.
- ***URLs**:* Lists URL(s) for this parent and indicates whether they are external or not.
- ***Version:*** Version number of the site/management server.
- ***Service account:*** The service account under which the management server is running.
- ***Time for last synchronization:*** Last synchronization date.
- ***Status for last synchronization:*** Status of last synchronization. It can be either *Successful* or *Failed*. If failed, further information is offered.

Due to synchronization issues, any changes made to remote children might take some time to be reflected in the *Site Navigation* pane. See Basic Rules of Federated Sites (on page 174).

Backup, Restore and Move System Configuration

Scheduled Backup & Restore of System Configuration

Regularly backing up your RC-E database is always recommended—especially if you have a larger RC-E setup. Having a scheduled regular backup provides you with an always up to date backup. In case of a disaster recovery scenario, regular backups limit your loss of data to what was changed since last backup. Furthermore, it offers you the ability to quickly restore your RC-E configuration. However, regularly backing up also has the added benefit that it flushes your Microsoft SQL Server's transaction log.

If you have a smaller RC-E setup and do not feel the need for regular scheduled backup, see Manual Backup & Restore of System Configuration (on page 185).

The management server stores your RC-E system's configuration in a database. When backing up/restoring management server(s), make sure that this database is included in the backup/restore.

Flushing the SQL Server Transaction Log

What Is the SQL Server Transaction Log and Why Does It Need to Be Flushed? Each time a change in the RC-E data occurs, the SQL Server will log this change in its transaction log - regardless whether it is a SQL Server on your network or a SQL Server Express edition. The transaction log is essentially a security feature that makes it possible to roll back and undo changes to the SQL Server database. The SQL Server by default stores its transaction log indefinitely, and therefore the transaction log will over time build up more and more entries. The SQL Server's transaction log is by default located on the system drive, and if the transaction log just grows and grows, it may in the end prevent Windows from running properly. Flushing the SQL Serve's transaction log from time to time is thus a good idea; flushing it does not in itself make the transaction log file smaller, but it prevents it from growing out of control. RC-E does not, however, automatically flush the SQL Server's transaction log at specific intervals. You can also do several things on the SQL Server itself to keep the size of the transaction log down. For numerous articles on this topic, go to support.microsoft.com (see http://support.microsoft.com/ - http://support.microsoft.com/) and search for SQL Server transaction log.

Prerequisites

SQL Server Express Edition users only: Microsoft® SQL Server Management Studio Express, a tool downloadable for free from www.microsoft.com/downloads (see http://www.microsoft.com/downloads - http://www.microsoft.com/downloads). Among its many features for managing SQL Server Express databases are some easy-to-use backup and restoration features. Download and install the tool on your management server.

Scheduled Back Up of System Configuration

1. Open Microsoft SQL Server Management Studio Express from Windows' *Start* menu by selecting *All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio Express*.
2. In the tool do the following:
3. When connecting, specify the name of the required SQL Server. Use the account under which the database was created.
    - Find the *Surveillance* database, containing your entire RC-E system configuration, including recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, etc.

No Surveillance database? Surveillance is the default name of the database containing the system configuration. If you can find the database, but it is not called Surveillance, it could be because you gave the database another name during the management server installation.

View example... We will assume that the database uses the default name.

Example: During management server installation it is possible to change the database name from the default name Surveillance to another name

- Make a backup of the *Surveillance* database and make sure to:
  - Verify that the selected database is *Surveillance*
  - Verify that the backup type is **full**
  - Set the schedule for the recurrent backup
  - Verify that the suggested path is satisfactory or select alternative path
  - Select to **verify backup when finished** and to **perform checksum before writing to media**.

4. Follow the instructions in the tool to the end.

Tip: Also consider backing up the *Surveillance Log* database, using the same method.

Backing Up Log Server Database

Handle the *SurveillanceLogServer* database using the same method as when handling system configuration described earlier in this topic. The *SurveillanceLogServer* database (name may be different if you renamed the system configuration database) contains all your OnSSI RC-E system logs, including errors reported by recording servers and cameras.

The database is located where the Log Server Service is installed, typically the same place as your management server. Backing up this database is not vital since it does not contain any system configuration, but you may later appreciate having access to system logs from before the management server backup/restore.

Restoring System Configuration (From Scheduled Back Up)

Prerequisite: To prevent configuration changes being made while you restore the system configuration database, stop the:

- Management Server Service (see "Management Server Service and Recording Server Service" on page 198)
- World Wide Web Publishing Service, also known as the Internet Information Service (IIS). Learn how to stop the IIS at: http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx (see http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx - http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx).

Open Microsoft SQL Server Management Studio Express from Windows' *Start* menu by selecting *All Programs* > *Microsoft SQL Server 2008* > *SQL Server Management Studio Express*.

1. In the tool do the following:
   - When connecting, specify the name of the required SQL Server. Use the account under which the database was created.
   - Find the *Surveillance* database, containing your entire RC-E system configuration, including recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, etc.
   - Make a restore of the *Surveillance* database and make sure to:

- Select to backup **from** device
- Select backup media type **file**
- Find and select your backup file *Surveillance.bak*
- Select to **overwrite the existing database**.

2. Follow the instructions in the tool to the end.

If you also backed up the *Surveillance Log* database from the old management server, restore it on the new management server using the same method.

Note that RC-E basically will not work while the Management Server Service (see "Management Server Service and Recording Server Service" on page 198) is stopped; it is thus important to remember to start the services again once you have finished restoring the database.

Manual Backup & Restore of System Configuration

Backing up your RC-E database is always recommended. In case of a disaster recovery scenario this offers you the ability to quickly restore your RC-E configuration. Furthermore, being able to easily do a manual backup of your entire system configuration via your Management Client (no need for third-party tools) offers you flexibility, security and full control of your configuration.

The type of backup described in this topic is best suited if you have a smaller RC-E setup and wish to do a one-time, non-scheduled backup. Besides manual backups, it is strongly recommended to also configure regular, scheduled system backups (see "Scheduled Backup & Restore of System Configuration" on page 183)—especially if you run a larger RC-E setup.

Select Shared Backup Folder

Before backing up and restoring any system configuration, you must set a backup folder for this purpose.

1. Right-click the notification area's management server service icon and select *Select shared backup folder...*
2. In the window that appears, browse to the wanted file location.
3. Click *OK* twice.
4. If asked if you want to delete files in the current backup folder, click *Yes* or *No* depending on your needs

Manual Back Up of System Configuration

Important information:

- Your RC-E system stays online
- A backup cannot be used for copying configurations to other RC-E installations, see Move System Configuration to New Management Server (on page 186) for details on this.
- Depending on your RC-E configuration, your hardware, and on whether your SQL server, management server and Management Client are installed on the same machine or not, backing up configuration might take some time.
- Logs (including Audit logs (see "Manage Logs" on page 158)) are **not** part of the configuration backup.

Backing up:

All relevant RC-E configuration files will be combined into one single .cnf file, which is saved at a specified location.

1. From the Management Client's menu bar, select *File, Backup Configuration....*
2. Next, you are presented with an important note. Read the contents of the note. Click *Backup.*
3. In the file save dialog, browse to the location where you want to store the configuration backup. Specify a suitable file name, and click *Save.*
4. Let the *Backup Configuration* window finish. Click *Close.* Your backup is finished.

Restoring System Configuration (From Manual Back Up)

Important information:

- Both the user installing and the user doing the restore must be local administrator on the management server **and** on the SQL server.
- Except for your recording servers, RC-E will be completely shut down for the duration of the restore, which might take some time.
- A backup can only be restored on the RC-E installation where it was created. Furthermore, make sure that the setup is as similar as possible to when the backup was made. Otherwise, the restore might fail.
- If restoring fails during the validation phase, it **will** be possible to start the old configuration again (since no change have been committed).
  If restoring fails elsewhere in the process, rolling back to the old configuration is impossible.
  As long as the backup file is not corrupted, it **will** however be possible to do another restore.
- Restoring replaces the current configuration. This means that any configuration changes since last backup is lost.
- No logs (including Audit logs (see "Manage Logs" on page 158)) are restored
- Once restoring has started, it cannot be canceled.

Restoring:

1. Right-click the notification area's Management Server service icon and select *Restore Configuration....*
2. Next, you are presented with an important note. Read the contents of the note. Click *Restore.*
3. In the file open dialog, browse to the location of the configuration backup file, select it, and click *Open.*
4. The *Restore Configuration* window will now run, showing progress and status information. Wait for it to finish and click *Close.* Your restore is finished.

Move System Configuration to New Management Server

It can sometimes be necessary to move the RC-E management server installation from one physical server to another. The management server stores your RC-E's system configuration in a database. If you are moving the management server from one physical server to another, it is vital that you make sure that your new management server also gets access to this database. The system configuration database can be stored in two different ways:

- **Network SQL Server:** If you are storing your RC-E system's configuration in a database on an existing SQL 2005 or 2008 Server on your network, you can simply point to the database's location on that SQL Server when installing the management server software on your new management server. In that case, only the following paragraph about management server hostname and IP address applies and you should ignore the rest of this topic:

  Management server hostname and IP address: When you move the management server from one physical server to another physical server, it is by far the easiest to give the new server the same hostname and IP address as the old one. This is due to the fact that the recording server will connect to the hostname and IP address of the old management server. In case the new management server has been given a new hostname and/or IP address, the recording server will not be able to find the management server. Manually stop each recording server in your system, change their management server URL, and when done, restart them.

- **SQL Server Express Edition:** If you are storing your RC-E system's configuration in a SQL Server Express Edition database on the management server itself, it is important that you back up the existing management server's system configuration database before the move. By backing up the database, and subsequently restoring it on the new server, you will avoid have to reconfigure your cameras, rules, time profiles, etc. after the move.

Some of this prerequisite information is only relevant for users of SQL Server Express Edition. **If you use any other SQL setup, ask your IT department for backup details.**

Prerequisites

- **Your RC-E software installation file for installation on the new management server**.

- **Your initial license (.lic) file**, i.e. the one you used when initially installing RC-E , not the .lic file which is the result of your license activation (see "Activate Licenses" on page 43). License activation is, among other things, based on the specific hardware on which the activation took place; therefore an activated .lic file cannot be reused when moving to a new server. Note that if you are also upgrading your RC-E software in connection with the move, you will have received a new initial .lic file together with your new Software License Code (SLC).

- **SQL Server Express Edition users only: Microsoft® SQL Server Management Studio Express**, a tool downloadable for free from www.microsoft.com/downloads. Among its many features for managing SQL Server Express databases are some easy-to-use backup and restoration features. Download and install the tool on your existing management server *and* on the server which will be your future management server (you will need it for the entire copy process (backup as well as restoration)).

  Management server hostname and IP address: When you move the management server from one physical server to another physical server, it is by far the easiest to give the new server the same hostname and IP address as the old one. This is due to the fact that the recording server will connect to the hostname and IP address of the old management server. In case the new management server has been given a new hostname and/or IP address, the recording server will not be able to find the management server. Manually stop each recording server in your system, change their management server URL, and when done, restart them.

Moving System Configuration:

Moving your system configuration is a three step process:

1. First you make a copy of your system configuration (identical to making a scheduled backup (see "Scheduled Backup & Restore of System Configuration" on page 183))

2. Then you install the new management server on the new server (see scheduled backup (see "Scheduled Backup & Restore of System Configuration" on page 183), step 2)

3. And finally you copy/restore your system configuration to the new system (see how to restore a scheduled backup (see "Scheduled Backup & Restore of System Configuration" on page 183))

Copying System Configuration from Old Server (Step 1)

Prerequisite: Stop the Management Server service (see "Management Server Service and Recording Server Service" on page 198) to prevent configuration changes being made. This is important since any changes made to the RC-E configuration, between the time you create a copy and the time you restore it on your new management server, will be lost. If changes are made after the copy was made, you will have to make a new copy.

Note that RC-E basically will not work while the Management Server service (see "Management Server Service and Recording Server Service" on page 198) is stopped; it is thus important to remember to start the service again once you have finished backing up the database.

Since first part of a copy is in reality identical to a scheduled backup, see Scheduled Back Up of RC-E System Configuration section (see "Scheduled Backup & Restore of System Configuration" on page 183), steps 1-3.

What Happens while the Management Server Is Unavailable?

- **Recording servers will still be able to record:** Any currently working recording servers will have received a copy of their configuration from the management server, so they will be able to work and store recordings on their own while the management server is down. Scheduled and motion-triggered recording will therefore work, and event-triggered recording will also work unless based on events related to the management server or any other recording server since these go through the management server.
- **Recording servers will temporarily store log data locally:** They will automatically send log data to the management server when the it becomes available again.
    - **Clients will not be able to log in:** Client access is authorized through the management server. Without the management server, clients will not be able to log in.
    - **Already logged in clients can remain logged in for up to an hour:** When clients log in, they are authorized by the management server and can communicate with recording servers for up to one hour. If you can get the new management server up and running within an hour, many of your users will not be affected.
    - **No ability to configure the system:** Without the management server, you will not be able to change system configuration.

Even though some users might not experience loss of contact, we recommend that you inform your users about the risk of losing contact with the surveillance system while the management server is down.

Copying Log Server Database

Handle the *SurveillanceLogServer* database using the same method as when handling system configuration described earlier in this topic. The *SurveillanceLogServer* database (name may be different if you renamed the system configuration database) contains all your OnSSI RC-E system logs, including errors reported by recording servers and cameras.

The database is located where the Log Server Service is installed, typically the same place as your management server. Backing up this database is not vital since it does not contain any system configuration, but you may later appreciate having access to system logs from before the management server backup/restore.

Installing New Management Server on New Server (Step 2)

Installing a management server (see "Install Management Server" on page 13) is divided into three steps. During step 2 of the installation on your new management server, make sure you select *Create a new database* for the system configuration database, even though you have a backup of the database from your old management server.

Next (see "Copying/Restoring System Configuration to New Server (Step 3)" on page 189), we must overwrite the new and empty database by restoring the backup we just created. Since we are going to overwrite the new and empty database, it is important that it has the same name as the backed-up database (if your backed-up database has the default name Surveillance, just use the default name *Surveillance* when creating the new database too).

The password for the database is not significant in this backup/restore context, but we recommend that you just use the default setting *Allow server to control password*.

Copying/Restoring System Configuration to New Server (Step 3)

Prerequisite: To prevent configuration changes being made while you restore the system configuration database, stop the:

- Management Server Service (see "Management Server Service and Recording Server Service" on page 198)

World Wide Web Publishing Service, also known as the Internet Information Service (IIS). Learn how to stop the IIS at: http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx (see http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx - http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx).

This should all be done to the **new** management server.

Since second part of a copy is in reality identical to a restore, see Restoring RC-E System Configuration (From Scheduled Back Up) (see "Restoring System Configuration (From Manual Back Up)" on page 186), steps 1-2 and rest of the topic for details.

Device Drivers

Manage and Remove Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to a recording server. The video device drivers should therefore be installed on each recording server on your RC-E system.

Video device drivers are installed automatically during the initial installation of your RC-E system. However, new versions of video device drivers are released and updated regularly on the OnSSI website.

Making New Video Device Driver Versions Available for Installation

The latest version of video device drivers is available for download from the OnSSI website.

Installing Video Device Drivers

1. On the computer running the recording server, shut down any OnSSI software, including the Recording Server service.
2. Download the new driver pack from www.onssi.com.
3. Run the executable. A wizard should be displayed.
4. Once the wizard is ready to install the video device drivers, click *Install* to complete the installation of the video device drivers.
5. When ready, start the Recording Server service again.

After restarting the Recording Server service, it might take several minutes for your hardware devices to make contact with the new drivers, so have patience. This is due to several internal checks being performed on the newly installed drivers.

Removing Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to a recording server. When the video device drivers are removed, communication between the recording server and the camera devices will no longer be possible.

To remove video device drivers — typically prior to installing a later version of the drivers — use the following procedure on the recording server computer on which the video device drivers are installed:

1. Open Windows' *Control Panel*, and select *Add or Remove Programs*. This will open the *Add or Remove Programs* window.
2. In the *Add or Remove Programs* window, select the *Video Device Driver Vx.x* entry (where x.x indicates the relevant version number), and click *Uninstall*.
3. You will be asked to confirm that you want to remove the video device drivers. Click *OK* to remove them.

Failover Servers

Failover Server Service Administration

When you have installed a failover server, you are able to check the state of the Failover Server service by looking at the Failover Server service icon in the notification area **of the computer running the failover server**. The notification area icon also lets you start and stop the Failover Server service, view status messages, etc.

Tip: The notification area is occasionally also known as the *system tray*, it is located at the far right of the management server computer's Windows taskbar.

While the Failover Server service is stopped, the failover server will not be able to take over from regular recording servers.

Starting and Stopping the Failover Server Service

The Failover Server service starts automatically. If you have stopped the service manually, you can start and stop it the following way:

1. Right-click the notification area's failover server icon.
2. From the menu that appears, select *Start Failover Server Service* or *Stop Failover Server Service*, depending on your needs.

Changing the Management Server Address

The failover server must be able to communicate with your RC-E system's management server. You therefore specify the IP address/hostname of the management server during the installation of the failover server.

Should you later need to change the address of the management server, you do it the following way:

In order to be able to change the management server address, the Failover Server service must be stopped.

1. Stop the Failover Server Service (see Starting and Stopping the Failover Server Service (on page 191)).
2. Right-click the notification area's Failover Server service icon again.
3. From the menu that appears, select *Change Settings...* The *Failover Recording Server Settings* window appears. You are able to change the following setting:
    - **Management server hostname / IP address:** Lets you specify the IP address (example: 123.123.123.123) or host name (example: ourserver) of the RC-E management server with which the failover server should be able to communicate.

Viewing Status Messages

1. Right-click the notification area's *Failover Server Service* icon.
2. From the menu that appears, select *Show Status Messages.* The *Failover Recording Server Status Messages* window appears, listing time-stamped status messages.

Viewing Version Information

Knowing the exact version of your *Failover Server Service* is an advantage if you need to contact product support.

1. Right-click the notification area's *Failover Server Service* icon.
2. From the menu that appears, select *About...*
3. A small dialog opens. The dialog will show the exact version of your *Failover Server Service.*

During installation of the failover server, you specified a user account under which the *Failover Server Service* should run. For the failover server to work, it is important that the user account in question has access to your OnSSI RC-E system with administrator rights.

To verify whether the user account has access to your OnSSI RC-E system, do the following:

1. In the Management Client's Site Navigation pane (see "Panes Overview" on page 36), expand *Security* and select *Roles*.
2. In the Overview pane (see "Panes Overview" on page 36)'s roles list, select the *Administrators* role.
3. In the Properties pane (see "Panes Overview" on page 36)'s role settings list, verify that the required user is listed.

   If the user is not listed, add the required user to the *Administrators* role by clicking the *Add...* button below the role settings list. For more information, see Assign Users & Groups to/from Roles (see "Assign and Remove Users and Groups to/from Roles" on page 149).

Manage Failover Servers

A failover server is a spare recording server which can take over if a regular recording server becomes unavailable. It should therefore always be installed on a separate computer. A failover server has two services:

- A Failover Server Service, which handles the processes of taking over from the regular recording server. By default, this service is always running since it constantly checks the state of relevant recording servers.
- A Recording Server Service, which enables the failover server to act as a recording server while the regular recording server is unavailable. This service is only started when required, i.e. when the failover server should take over from the regular recording server. Starting this service typically takes a couple of seconds, but may take longer depending on local security settings, etc.

A failover server **must** be able to communicate with all cameras of the recording server(s) from which it should be able to take over.

Involved Servers:

1. Recording server
2. Failover server
3. Management server

Failover Steps:

1. To check whether it is running or not, failover server has a non-stop TCP connection to a recording server.
2. This connection is interrupted, i.e. the recording server is not running.

3. From the management server, the failover server requests the current configuration of the recording server.
4. The management server sends the requested configuration and the failover server starts recording instead of the recording server.
5. The failover server and the relevant camera(s) exchange video data.
6. The failover server continually tries to re-establish connection to the recording server.
7. When the connection to the recording server is reestablished, the failover server shuts down and the recording server fetches video data (if any) recorded during its down-time.

Installing Failover Servers

For information about installing failover servers, see Recording Servers (on page 18).

Adding and Grouping Failover Servers

Failover servers are installed through an installation wizard, just like regular recording servers; see Installing Failover Servers (on page 193).

Overview of Failover Servers in Management Client

Once failover servers are installed, they become visible in the Management Client: In the Site Navigation pane (see "Panes Overview" on page 36), select *Servers,* then *Failover Servers* and view a list of installed failover servers in the Overview pane (see "Panes Overview" on page 36).

Tip: If a failover server does not become visible in the Management Client, verify that the failover server has been configured with the correct IP address/hostname of the management server. Also verify that the user account under which the Failover Server Service runs has access to your RC-E system with administrator rights.

Failover Servers Are Grouped

Failover servers are always grouped; a group can contain one or more failover servers. Grouping has a clear: When you later specify which failover servers should be able to take over from a recording server, you do not select a particular failover server; rather you select a group of failover servers. If the selected group contains more than one failover server, this gives you the security of being able to have more than just one failover server ready to take over if the recording server becomes unavailable.

Initially, your failover servers will all appear in the group *Unused Failover Servers*.

A red **x** on a failover server icon indicates that the failover server in question is currently not in use.

Creating Failover Groups

You can create as many new failover groups as required: In the Overview pane, right-click *Failover Groups* and select *Add Group* from the menu that appears.

Specify a name and a description (optional) of your new group, then click *OK*.

Adding Failover Servers to a Group

In the Overview pane, right-click the group to which you want to add one or more failover servers, then select *Edit Group Members* from the menu that appears. This will open the *Select Group Members* window. From the *Available* box in window's left side, select the required failover servers(s), then click *Add* to move the selected failover server(s) to the *Selected* box in the right side of the window:

Tip: Alternatively, drag and drop failover servers between the two boxes.

When ready, click *OK*. The required failover servers now belong to the group.

A failover server can only be a member of one group at a time.

Editing Failover Group Properties

Select the required failover group in the Overview pane.

- On the *Info* tab, you can edit the name and description of the selected failover group.
- On the *Sequence* tab, you can edit the sequence in which failover servers within the group should take over from unavailable recording servers.

Enabling Failover Servers

A failover server must be enabled before it will be able to take over from regular recording servers:

1. In the Overview pane (see "Panes Overview" on page 36), select the required failover server.
2. In the Properties pane (see "Panes Overview" on page 36), select *Enable this failover server*.

Editing Failover Server Properties

1. In the Overview pane, select the required failover server.
2. On the *Info* tab in the Properties pane, you are able to edit the following:
   - ***Name:*** Name of the failover server, as it will appear in the Management Client, in logs, etc.
   - ***Description:*** Optional description of the failover server, for example a description of the server's physical location.
   - ***Host name:*** Non-editable field displaying the network address of the failover server.
   - ***UDP port:*** The port number used for communication between failover servers. By default, port 8844 is used.

     Tip: The port used by the failover server for polling (i.e. regularly checking) the state of relevant recording servers is by default port number 11000. If required, you can change that port number on the recording server's *Failover* tab (see "Failover Tab (Recording Server Properties)" on page 64).
   - ***Database location:*** This field specifies the path to the database which the failover server should use for storing recordings while taking over from a regular recording server. When the regular recording server becomes available again, recordings stored by the failover server will be transferred to the regular recording server, and merged with recordings there.

     The database path cannot be changed while the failover server is taking over from a regular recording server. Changes you make will be applied when the failover server is no longer taking over from a regular recording server.
   - ***Enable this failover server:*** A failover server must be enabled before it will be able to take over from regular recording servers. Select box to enable the failover server, clear box to disable it.

     IMPORTANT: A disabled failover server will not be able to take over from regular recording servers.

3. On the *Network* tab, you are able to define the failover server's public IP address, etc. This is relevant especially if using NAT (Network Address Translation) and port forwarding. See the description of a regular recording server's *Network* tab (see "Manage Public Addresses" on page 72) for more information.

4. In the toolbar (see "Management Client Overview" on page 34), click *Save*.

Assigning Failover Servers to Recording Servers

In the Management Client, you select a recording server, then use the *Failover* tab (see "Failover Tab (Recording Server Properties)" on page 64) to specify which failover group(s) should take over from the recording server in question. On the *Failover* tab, you even have the flexibility of being able to assign a primary and a secondary failover group to each recording server.

Frequently Asked Questions

How does a failover server know when to take over? It polls (i.e. regularly check the state of) relevant recording servers every 0.5 seconds. If a recording server does not reply within 5 seconds after it was polled, the recording server is considered unavailable and the failover server takes over.

How long does it take for a failover server to take over? It takes 5 seconds plus the time it takes for the failover server's Recording Server Service to start. During this period it will not be possible to store recordings, neither will it be possible to view live video from affected cameras.

What happens when a recording server becomes available again? When it becomes available again, it will automatically take over from the failover server, and recordings stored by the failover server will automatically be merged into the regular recording server's databases.

How long the merging process takes will depend on the amount of recordings to merge, on network capacity, etc.

During the merging process, it will not be possible to browse recordings from the period during which the failover server took over.

What if the failover server must take over from another recording server during the merging process? In that case, it will postpone the merging process with recording server A, and take over from recording server B. When recording server B becomes available again, the failover server will take up the merging process with recording server A, after which it will begin merging with recording server B.

Will I lose recordings? A failover solution does not provide complete redundancy. It is, however, a very reliable way of minimizing downtime.

When the regular recording server becomes available again, the Failover Server Service will make sure that the recording server is ready to store recordings again. Only then is the responsibility for storing recordings handed back to the regular recording server. Thus, loss of recordings at this stage of the process is negligible.

How will clients experience failover? Clients should hardly notice that a failover server is taking over, although there will be a short period—usually only some seconds—with no access to video from the affected recording server while the failover server is taking over.

Clients will be able to view live video as soon as the failover server has taken over.

Clients will be able to play back recent recordings, i.e. recordings from after the failover server took over, since those recordings will be stored on the failover server. Clients will not be able to play back older recordings stored only on the affected recording server until that recording server is functioning again, and has taken over from the failover server.

Clients will, however, be able to access archived (see "About Storage and Archiving" on page 56) recordings stored at accessible locations, such as on available network drives, but clients will not be able to access archived recordings stored at inaccessible locations, such as on the unavailable recording server itself or on an unavailable network drive.

When the recording server is functioning again, there will usually be a merging process during which recordings made by the failover server are merged back into the recording server's database. During that merging process, clients will not be able to play back recordings from the period during which the failover server took over.

Is there a failover solution for failover servers? Setting up one failover server as backup for another failover server is not necessary. This is because you do not allocate particular failover servers to take over from a regular recording server; rather you allocate failover groups.

A failover group must contain at least one failover server, but you can add as many failover servers as required to a failover group. Provided a failover group contains more than one failover server, there will be more than one failover server capable of taking over from the regular recording server.

For more information about selecting the failover groups you require for a recording server, see the description of the Management Client's Failover tab (see "Failover Tab (Recording Server Properties)" on page 64).

Will archiving work while a failover server has taken over? Any archiving (see "About Storage and Archiving" on page 56) will work even when a failover server has taken over from a regular recording server, provided the archiving destination is on a network location accessible by the failover server.

If the archiving destination is inaccessible—such as on the unavailable recording server itself or on an unavailable network drive—archiving will not work as long as the destination is unavailable.

Failover-Related Events

OnSSI RC-E features two failover-related events, *Failover Started* and *Failover Stopped*, which you can use when creating rules (see "Manage Rules" on page 133). The two events are further described in the Events Overview (on page 128).

Database Corruption

Protect Databases from Corruption

If a recording server's databases become corrupted, the recording server is in many cases able to repair the corrupt databases. While the ability to repair corrupt databases is highly valuable, it is of course even better to take steps to ensure that your databases do not become corrupted:

Power Outages: Use a UPS

The single most common reason for corrupt databases is the recording server being shut down abruptly, without files being saved and without the operating system being closed down properly. This may happen due to power outages, due to somebody accidentally pulling out the server's power cable, or similar.

The best way of protecting your recording servers from being shut down abruptly is to equip each of your recording servers with a UPS (Uninterruptible Power Supply).

The UPS works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

Selecting the right type of UPS for your organization's environment is an individual process. When assessing your needs, however, do bear in mind the amount of runtime you will require the UPS to be able to provide if the power fails; saving open files and shutting down an operating system properly may take several minutes.

Windows Task Manager: Be Careful when Ending Processes

When working in Windows Task Manager, be careful not to end any processes which affect the surveillance system. If you end an application or system service by clicking *End Process* in the Windows Task Manager, the process in question will not be given the chance to save its state or data before it is terminated. This may in turn lead to corrupt camera databases.

Windows Task Manager will typically display a warning if you attempt to end a process. Unless you are absolutely sure that ending the process will not affect the surveillance system, make sure you click *No* when the warning message asks you if you really want to terminate the process.

Hard Disk Failure: Protect Your Drives

Hard disk drives are mechanical devices, and as such they are vulnerable to external factors. The following are examples of external factors which may damage hard disk drives and lead to corrupt camera databases:

- Vibration (make sure the surveillance system server and its surroundings are stable)
- Strong heat (make sure the server has adequate ventilation)
- Strong magnetic fields (avoid)
- Power outages (make sure you use a UPS; see more information in the previous)
- Static electricity (make sure you ground yourself if you are going to handle a hard disk drive).
- Fire, water, etc. (avoid)

Services Administration

Management Server Service and Recording Server Service

When the RC-E management server software is installed, you are able to check the state of the Management Server Service by looking at the *Management Server Service* icon in the notification area **of the computer running the management server**.

Likewise, when the RC-E recording server software is installed, you are able to check the state of the Recording Server Service by looking at the *Recording Server Service* icon in the notification area of the computer running the recording server in question.

The notification area icon also lets you start and stop the Management Server Service/Recording Server Service, view status messages, etc.

Tip: The notification area is also known as the *system tray.* It is located at the far right of the management / recording server's Windows taskbar.

IMPORTANT: When the **Recording Server Service** is running, it is **very** important that neither Windows Explorer nor other programs are accessing Media Database files or folders associated with your OnSSI RC-E surveillance setup. Otherwise, the recording server might not be able to rename or move relevant media files. Unfortunately, this might bring the recording server to a halt. If this situation has already occurred, stop the Recording Server Service, close the program accessing the media file(s) or folder(s) in question, and simply restart the Recording Server Service.

Accessing the Server Service

1. Right-click the notification area's Server Service icon.
2. From the menu that appears, depending on server type, select the needed icon.

If using multiple instances (see "Multiple Recording Server Instances" on page 26) of the Recording Server Service, a sub-menu lets you select whether you want to start a particular instance or all instances.

Starting the Server Service

1. See Accessing the Server Service (on page 198).
2. Select either *Start Management Server Service* or *Start Recording Server Service*.

Stopping the Server Service

While the recording server service is stopped, RC-E will not be able to interact with devices connected to the recording server. Consequently, no live viewing or recording will be possible.

While the management server service is stopped, you will not be able to use the RC-E Management Client at all.

1. See Accessing the Server Service (on page 198).
2. Select either *Stop Recording Server Service* or *Stop Management Server Service*.

Changing Recording Server Settings

To change basic settings for the Recording Server Service, such as which port numbers to use, do the following:

In order to be able to change settings, the Recording Server Service must be stopped. While the Recording Server Service is stopped, RC-E will not be able to interact with devices connected to the recording server. Consequently, no live viewing or recording will be possible.

1. See Accessing the Server Service (on page 198).
2. Select *Stop Recording Server Service*.
3. Right-click the notification area's recording server icon.
4. From the menu that appears, select *Change Settings...*

   The *Recording Server Settings* window appears. Change the appropriate settings.

Viewing Status Messages

1. See Accessing the Server Service (on page 198).
2. Select *Show Status Messages*.

   Depending on the current server type, either the *Management Server Status Messages* or *Recording Server Status Messages* window appears, listing time-stamped status messages.

Viewing Version Information

Knowing the exact version of your management server service or recording server service is an advantage if you need to contact product support.

1. In Management Client's menu bar select *Help* menu, click *About...*.
2. A small dialog opens. The dialog will, depending on server type, show the exact version of your management server service or recording server service.

Work with Recording Server Settings in details

- **Management server hostname / IP address:** IP address (example: 123.123.123.123) or host name (example: ourserver) of the RC-E management server to which the recording server should be connected. This information is necessary in order for the recording server to be able to communicate with the management server.
- **Management server port:** Port number to be used when communicating with the RC-E management server. Default is port 9993, although changeable if required.
- **Web server port:** Port number to be used for handling web server requests, for example for handling PTZ camera control commands and for browse and live requests from Ocularis Clients. Default is port 7563, although changeable if required.
- **TCP information port:** Port number to be used when the recording server listens for TCP information (some devices use TCP for sending event messages). Default is port 5432, although changeable if required.
- **SMTP server port:** Port number to be used when the recording server listens for SMTP information (some devices use SMTP (e-mail) for sending event messages). Default is port 25, although changeable if required.
- **FTP server port:** Port number to be used when the recording server listens for FTP information (some devices use FTP for sending event messages. Default is port 21, although changeable if required.

Virus Scanning

Virus Scanning Information

Virus scanning should in some cases be avoided—if allowed in your organization.

If you use virus scanning software on:

- recording data in databases on recording servers
- data being archived in archiving (see "About Storage and Archiving" on page 56) locations

it will most likely use a considerable amount of system resources on scanning.

This may affect system performance negatively, notably scanning of data in databases containing recordings. Some virus scanning software may furthermore temporarily lock each file it scans, which may further impact system performance negatively. Virus scanning may even corrupt recording databases, and render your surveillance system recordings useless.

Therefore:

- Do not use virus scanning on recording server directories containing recording databases (by default C:\MediaDatabase\ and all folders under that location, but note that different recording paths may have been specified in your organization).
- Do not use virus scanning on archiving locations.
- Do not use virus scanning on files with the following file extensions (which are all surveillance system-related):
    - .blk
    - .idx
    - .pic
    - .pqz
    - .sts
    - .ts
- Do not use virus scanning on the management server.

Your organization may have strict guidelines reg. virus scanning, but it is important that the mentioned locations and files are exempt from virus scanning. If allowed, you should therefore disable any virus scanning of recording servers' databases, of any archiving locations as well as on the management server. Consult your organization’s IT system administrator if in doubt.

SNMP

SNMP Support

OnSSI RC-E supports SNMP (Simple Network Management Protocol), a standard protocol for monitoring and controlling network devices, for managing their configuration, or collecting statistics, etc.

OnSSI RC-E will act as an SNMP agent, which can generate an SNMP trap as a result of a triggered rule. A third party SNMP management console can then receive information about the rule-triggering event, and operators of the SNMP management console can configure their system for further action as required.

The implementation uses Microsoft Windows SNMP Service for triggering SNMP traps. The SNMP Service must therefore be installed on recording servers. This will—when the SNMP Service has been configured through its own user interface—enable recording servers to send .mib (Management Information Base) files to the SNMP management console.

Installing the SNMP Service

1. On the required recording servers, open Windows' *Add or Remove Programs* dialog (*Start* > *Control Panel* > *Add or Remove Programs*).
2. In the left side of the *Add or Remove Programs* dialog click *Add/Remove Windows Components*. This will open the *Windows Components* wizard.
3. In the wizard, select the check box next to *Management and Monitoring Tools*, then click *Details...* to open the *Management and Monitoring Tools* dialog.
4. In the *Management and Monitoring Tools* dialog, select the check box next to *Simple Network Management Protocol*, then click *OK*.
5. Back in the *Windows Components* wizard, click *Next* and follow the wizard's further steps.

Configuring the SNMP Service

1. On the required recording servers, select *Start* > *Control Panel* > *Administrative Tools* > *Services*.
2. Double-click the SNMP Service.
3. Select the *Traps* tab.
4. Specify a community name, and click *Add to list*.
5. Select the D*estinations* tab.
6. Click *Add*, and specify the IP address or host name of the server running your third party SNMP management station software.
7. Click *OK*.

Daylight Saving Time

Daylight Saving Time

Daylight saving time (DST) is the practice of advancing clocks in order for evenings to have more daylight and mornings to have less. Typically, clocks are adjusted forward one hour sometime during the spring season and adjusted backward sometime during the fall season, hence the saying *spring forward, fall back*. Note that use of DST varies between countries/regions.

When working with a surveillance system, which is inherently time-sensitive, it is important to know how the system handles DST.

Spring: Switch from Standard Time to DST

The change from standard time to DST is not much of an issue since you jump one hour forward. Typically, the clock jumps forward from 02:00 standard time to 03:00 DST, and the day thus has 23 hours. In that case, there is simply no data between 02:00 and 03:00 in the morning since that hour, for that day, did not exist.

Fall: Switch from DST to Standard Time

When you switch from DST to standard time in the fall, you jump one hour back. Typically, the clock jumps backward from 02:00 DST to 01:00 standard time, repeating that hour, and the day thus has 25 hours.

Server-side Handling

OnSSI RC-E uses Coordinated Universal Time (UTC), which is the official world reference for time. UTC is not adjusted to reflect switches either to or from DST. Since RC-E uses UTC, no RC-E recordings are ever stored with the same timestamp twice, not even during the DST change hour.

Viewing DST Change Hour Recordings in Clients

When you want to view recordings from the last (most recent) hour of the DST change hour, simply go ahead and view them.

When you want to view recordings from the first hour of the DST change hour, do the following:

1. On the computer on which the client is used, go to Windows' *Start* menu, and select *Control Panel*.
2. In the Control Panel, double-click *Date and Time*.
3. In the *Date and Time Properties* window, select the *Time Zone* tab.
4. Make sure the *Automatically adjust clock for daylight saving changes* check box is cleared, then click *OK*.

When the Automatically adjust clock for daylight saving changes check box is cleared, recordings from the entire DST period will be Standard Time (or one hour off compared to DST). This means that recordings from the first hour of the DST change hour can now be viewed.

IMPORTANT: When you are done viewing recordings from the first hour of the DST change hour, select the Automatically adjust clock for daylight saving changes check box again to avoid confusion. We recommend not to clear the Automatically adjust clock for daylight saving changes check box unless you specifically need to view recordings from the first hour of the DST change hour.

Contact Information

On-Net Surveillance Systems (OnSSI)

One Blue Plaza
7th Floor
P.O. Box 1555
Pearl River, NY 10965

Website:	www.onssi.com	
General:	info@onssi.com	845.732.7900
Fax:		845.732.7999
Sales Support:	sales@onssi.com	845.732.7900 x 1
PreSales Support	salesengineering@onssi.com	845.732.7900 x 2
Technical Support:	support@onssi.com	845.732.7900 x 3
Training:	training@onssi.com	845.732.7900 x 4
Marketing:	marketing@onssi.com	845.732.7900 x 5